CPNI
Centre for the Protection
of National Infrastructure

INTRUSION DETECTION SYSTEMS

GUIDANCE FOR SECURITY MANAGERS

July 2013

This document has been produced by BRE Global Ltd as part of a programme of research and development funded and directed by the Centre for the Protection of National Infrastructure (CPNI). It provides security managers and Departmental Security Officers (DSOs) with guidance and information on the selection, commissioning, use and maintenance of intrusion detection systems. Used in conjunction with the Catalogue of Security Equipment (CSE) it will help with the development of an intrusion detection system operational requirement (OR).

Following the guidance in this document does not in itself confer immunity from legal obligations. It is the responsibility of the user to ensure they possess the latest issue and all amendments.

Contents

Introduction

The purpose of this document is to inform security managers, Departmental Security Officers (DSOs) and those responsible for determining the operational requirements of intrusion detection systems (IDS), and those who ensure that performance of the systems is maintained.

The guidance given relates to electronic IDS intended for indoor use. It includes good practice advice on installation, commissioning, operation and the maintenance necessary to keep the IDS system operating effectively and reliably. The concepts behind intrusion detection, the technologies used and how they should be applied are explained.

Key information is marked by the following symbols:

☞	'Must read' information
⚠	Cautionary Note
💡	Useful information or tip

Throughout this document reference is made to security managers but also includes DSOs and other persons responsible for the correct operation of intrusion detection systems.

Security managers new to the role should find the guidance a helpful starting point, whilst those more experienced will have a useful source of reference.

Before attempting to write a performance specification for a new intrusion detection system, it is important to ensure that a comprehensive operational requirement (OR) has been produced to provide the necessary details about the requirement.

This document does not include guidance on writing operational requirements, however advice can be found in CPNI's *Guide to Producing Operational Requirements for Security Measures*[1].

The information in Annex A and B is provided for those interested in knowing more about detection technology and warning device types.

Abbreviations

ACE	Ancillary Control Equipment
AIR	Active Infrared
ARC	Alarm Receiving Centre
ATE	Alarm Transmission Equipment
ATP	Alarm Transmission Path
ATS	Alarm Transmission System
BT	British Telecom
BUS	Binary Unit System
CCTV	Closed Circuit Television
CIE	Control and Indicating Equipment
CPTED	Crime Prevention through Environmental Design
CSV	Comma Separated Variable
DSO	Departmental Security Officer
EMC	Electromagnetic Compatibility
EN	European Norm
GPRS	General Packet Radio Services
GSM	Global System for Mobile Communications
HD	Hold-up device
I&HAS	Intrusion and Hold-up Systems (As used by the European EN standards)
IDS	Intrusion Detection System
LED	Light Emitting Diode
LVD	Low Voltage Directive
NSI	National Security Inspectorate
OR	Operational Requirement
PD	Published Document (a document published by BSI which is not a standard)
PIR	Passive Infrared
PSU	Power Supply Unit
RCT	Receiving Centre Transceiver
SAB	Self-actuating Bell
SCB	Self-contained Bell
SNE	Site Network Equipment
SPT	Supervised Premises Transceiver
SSAIB	Security Systems and Alarm Inspections Board
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol

Theory and concepts of Intrusion Detection Systems

Basic principles

The primary purpose of an intrusion detection system is to detect and signal the presence of an intruder or an intrusion attempt into a secured area. A secured area can be a selected room, an entire building, or group of buildings. The term 'supervised area/premises' is used in this guide to describe the protected area or building.

In principle, a basic intruder detection system will comprise a means to interface with the system user(s), e.g. a keypad with alpha-numeric display permitting authorised persons to interact with the system by setting and un-setting the IDS and viewing status indications.

Control electronics connected to the user interface will perform the set and unset functions and will have provision to receive inputs from detection devices distributed throughout the supervised area/premises in strategically located positions. The action of signalling the intrusion event (or to use the correct terminology, ‘to notify’) is also made by the control electronics.

In practice the component parts of an IDS are normally housed in discrete enclosures, although in theory other configurations are possible and IDS of the future may be integrated into other types of equipment, such as building control modules, light fittings and other fixtures. However, for the foreseeable future, there will continue to be a discrete control panel housing the control/processing electronics and, usually, a power supply.

The system will have one or more detectors and at least one means of raising the alarm. This may be an audible siren, visible indicator (e.g. a strobe light) or a transceiver capable of sending an electronic signal or message to a monitoring centre or guarding force located either at the supervised premises or on another site remote from the supervised premises.

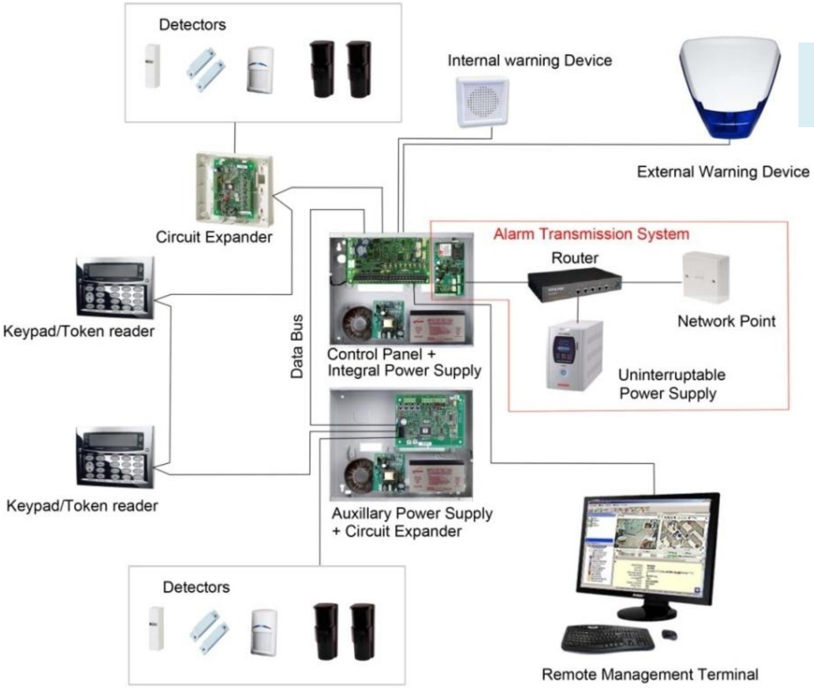


Figure 1: Schematic showing the components of a typical intrusion detection system

Reliable operation

The most important aspect of any intruder detection system is its reliability. A significant step towards achieving a reliable system is selecting equipment and components which are compatible with the service environment. Equally important is to position and configure the equipment correctly to provide the desired performance. Motion detectors capable of detecting minute emissions of heat energy radiating from the body of an intruder are also expected to tolerate the climatic changes that may occur between the temperature extremes of the day and the night without creating a false alarm. Technology can make such demanding requirements possible, but good installation practice must be followed to ensure an acceptable level of reliability is achieved in service.

An acceptable balance between false alarm immunity and the rapid detection of an intruder must be found. If a suitable balance cannot be achieved, the OR may need to be revised. Where conflicts of opinion exist regarding the most effective compromise, it is recommended that performance be demonstrated before any significant commitment is made.

The intrusion detection system will normally be designed to provide the earliest possible warning of an intrusion attempt. Securing a premises or area against unauthorised entry requires physical protection, using suitably robust fences, barriers, walls, and doors etc. Physical security serves to prevent or at least delay entry. Electronic intrusion detection systems on the other hand are intended to provide the means to detect and signal unauthorised entry attempts in sufficient time to permit the response force to arrive before the physical barriers are breached, or where only limited access to the protected area has been achieved.

Defence in Depth

It is good practice to implement protection in layers. This approach is often referred to as an ‘onion skin’, requiring the penetration of multiple protective measures before assets of any significance can be reached. The concept of layering is applicable to both the implementation of physical security measures and the intrusion detection system components. Indeed it should be considered an essential feature of security protection because individual components will have their specific strengths and weaknesses but when used together to form a complete system the weaknesses take on less significance.

The application of security measures must be tailored to the needs of the facility to be secured. The security approach will be influenced by the type of facility, the nature of the assets to be protected, previous experience and the perceived threats and vulnerabilities. These parameters must be identified by the completion of an Operational Requirement (OR) which provides a statement of the overall security need. It is from the OR that the basic criteria and specification for the intrusion detection system can be determined.

The type of intrusion detection system installed and the technologies deployed depends upon the level of security required, the environment in which the intrusion detection components are to be used and the activities undertaken within the secured area(s). The aim is to achieve a high probability of detection of intruders, with a minimum of false alarms and as far as possible, the least disruption to legitimate users.

CPNI Grading structure

To guide security managers in their choice and recommendations, CPNI grades both systems and components. Two methods of grading IDS are in place and their use is dependent upon the nature of the asset and the perceived threat.

The **CPNI Class Rating system** is to be used to protect protectively marked material against undetected compromise.

The **CPNI Protection Level system** is to be used to protect all assets against theft and damage.

The table below specifies the intent of the attack or threat to be countered in relation to the type of asset being protected and designates which CPNI grading system should be applied.

Table 1: CPNI grading matrix

		Attack Purpose		
		Undetected Compromise of Asset	Asset Theft	Asset Damage
Asset Type	Information	Class	Protection	Protection
	People	N/A	N/A	Protection
	Buildings	N/A	N/A	Protection
	Equipment	Class	Protection	Protection

The choice of a particular Protection Level for protecting assets from theft and/or damage will be based on the Operational Requirement approach. The selection of the appropriate CPNI Class Rating for products or systems will be based on a risk assessment as described in the security Policy Framework, (SPF)[2] using security Assessment for protectively Marked Assets (SAPMA)[3] in conjunction with an OR-based methodology.

Selection of the appropriate CPNI Protection Level for products or systems will be made following the production of a detailed Operational Requirement (Level 1 and Level 2). Consult CPNI for advice on the appropriate Protection Level for the elements to be deployed.

Product and system requirements to meet the specific CPNI grading are contained within published CPNI Standards. Consideration is given to the likely knowledge and skills of an attacker, the availability of tools or equipment the attacker may employ together with the likelihood of an attack leaving visible evidence. A view is also taken regarding false alarms which cause the system to be discredited. It is recognised that for installed systems, factors which influence this include the provision of alarm confirmation (e.g. CCTV) together with the motivation of the guard force.

Products successfully demonstrating compliance against these standards are listed in the Catalogue of Security Equipment (CSE)[4]. Selection of products from the CSE should be supported by a performance specification appropriate to the specific application/installation.

Standards and regulations

Standards

The former British Standards BS 4737[5], BS 7042[6] and BS 6799[7] which were used to govern the specification, installation and maintenance of IDS in the UK were withdrawn on 1 October 2005 in favour of a common set of European 'EN' standards (i.e. European norms). These have now become the accepted minimum requirement for IDS across Europe. The implementation in the UK was defined in PD 6662[8], which also included elements omitted from the European standards such as maintenance requirements.

The main set of European norms applicable to IDS is the EN 50131 series, which has been adopted by British Standards and re-labelled BS EN 50131[10].

BS EN 50131 is one of a family of standards which were created to make it easier for security equipment manufacturers to sell products in all EU countries and permit security installation companies and engineers to work across borders in those countries. The standards also provide more visibility and understanding for customers in order to judge the quality of products sourced from anywhere within the European Union.

The standards applicable to electronic security equipment are:

BS EN 50130 - Environmental and EMC requirements
BS EN 50131 - Intrusion systems
BS EN 50132 - CCTV
BS EN 50133 - Access Control
BS EN 50134 - Social Alarms
BS EN 50135 - Hold-Up Alarms
BS EN 50136 - Alarm Transmission Systems
BS EN 50137 - Combined or Integrated Systems

BS EN 50131 comprises:

BS EN 50131-1 - General Requirements
BS EN 50131-2 - Intrusion Detectors
BS EN 50131-3 - Control and Indicating Equipment
BS EN 50131-4 - Warning Devices
BS EN 50131-5 - Interconnections
BS EN 50131-6 - Power Supplies
BS EN 50131-7 - Application Guidelines
BS EN 50131-8 - Security Fog devices
BS EN 50131-9 - Alarm verification - Methods and principles

Full titles and references of the sub parts can be found in the *References* section of this document.

In addition to the standards listed, there is a legal obligation for equipment manufacturers to ensure their products comply with the electrical safety and electromagnetic compatibility requirements of the applicable EU Directives, see *Regulations for Components*.

Commercial alarm systems

BS EN 50131-1[10] sets out four classifications of environmental performance levels (i.e. Class I to Class IV). These are representative of conditions ranging from benign indoor to exposed outdoor locations. Refer to *Environmental considerations* for further guidance.

To avoid confusion, it is strongly recommended that the OR clearly distinguishes between the classification of environmental performance of BS EN 50131-1[10] and the Class Ratings 1 to 4 of the CPNI grading system.

The BS EN 50131-1[10] standard also defines four security grades (i.e. Grade 1 to Grade 4):

Grade 1: Low risk - an intruder or robber is expected to have little knowledge of I&HAS and be restricted to a limited range of easily available tools.

Grade 2: Low to medium risk - an intruder or robber is expected to have a limited knowledge of I&HAS and the use of a general range of tools and portable instruments (e.g. a multi-meter).

Note: The PD 6662 scheme in the UK also permits Grade 2 'X', a variation of Grade 2 where the IDS has audible warning devices but is not monitored by an ATS.

Grade 3: Medium to high risk - an intruder or robber is expected to be conversant with I&HAS and have a comprehensive range of tools and portable electronic equipment.

Grade 4: High risk - to be used when security takes precedence over all other factors. An intruder or robber is expected to have the ability or resource to plan an intrusion or robbery in detail and have a full range of equipment including means to substitute components in an I&HAS.

Typically there are only two grades commonly adopted in the UK: Grade 2X for 'bells only' systems (usually implemented for domestic application), and Grade 3 for remotely monitored systems (the minimum insurance standard for high value domestic risk and commercial systems).

Introduction of European Standards within the UK

To help align BS EN 50131, Part 1- *System requirements*[10] with the practices of the UK intruder alarm industry, the European requirements are supplemented by PD 6662[8]. Both documents are used in conjunction with the application guidelines of DD CLC/TC 50131-7[9].

Companies accredited under installer schemes operated by the UK inspectorates, such as NSI and SSAIB, will have their installations inspected for compliance with BS EN 50131-1[10] and PD 6662[8] or where appropriate, the CPNI gradings.

It is not necessary for the security manager to obtain all parts of the BS EN 50131 series of standards. It is recommended that BS EN 50131-1 - System Requirements[10], DD CLC/TS 50131-7[9] - Application guidelines, PD 6662[8], BS 8243[13], BS 8473[15] and DD 263[14] are purchased. These documents form the basis of the requirements for IDS installations within the UK.

Supervised premises transceivers shall as a minimum, conform to the requirements of the appropriate parts of BS EN 50136 - Alarm Transmission Systems[20] as specified by BS EN 50131-1[10].

Component grading

The security grading and environmental classification systems of EN50131 should not be confused with the CPNI Protection Levels and Class Ratings, they are different. However, the EN and CPNI systems complement one another; for example, the requirements for the CPNI Protection Levels build upon the performance requirements associated with EN security grade 3 and in some instances, EN security grade 4.

Compliance with the relevant EN security grade 3 standards must be demonstrated as a prerequisite for listing IDS components in the Catalogue of Security Equipment. Intrusion equipment that has been self-certified by the equipment manufacturer or supplier is not accepted.

IDS components required for use with applications designated as requiring CPNI Protection Level ENHANCED or HIGH and all CPNI Class Ratings shall also have been tested to, and have met the requirements of the applicable CPNI IDS standards. See page 56.

IDS components for use with applications designated as requiring Protection Level BASE shall as a minimum, require evidence of compliance with the relevant EN security grade 3 requirements. Acceptable evidence shall be an approval certificate or test report from an accredited certification body/test laboratory that is independent from the equipment manufacturer/supplier.

CPNI

Standard for Intrusion Detection Systems

Passive Infrared Detectors

Requirements for listing in the
Catalogue of Security Equipment

Standard for Intrusion Detection Systems
Passive Infrared Detectors

Figure 2: Example CPNI - IDS Standard

Regulations for components

Unlike fire detection equipment, the performance standards and requirements associated with IDS are not mandated, meaning that manufacturers of IDS equipment do not need to demonstrate compliance with the EN 50131 standards in order to CE mark their products.

The exceptions are the electrical safety requirements and electromagnetic compatibility of the LVD[11] and EMC[12] Directives respectively. There is a legal obligation for IDS manufacturers to confirm that the requirements prescribed by these directives have been fulfilled; applying the CE mark on the product is a declaration that they have.

The manufacturer must produce a technical construction file for each product in which justification is made describing how compliance is achieved. Alternatively the manufacturer may choose to have the products independently tested to confirm compliance.

It should be noted that compliance with the LVD[11] and EMC[12] Directives is applicable to the IDS components as they were placed on to the market. The fitting of other IDS devices/modules into the enclosures of compliant equipment may invalidate that compliance. An example could be the fitting of a supervised premises transceiver (SPT) into a control panel enclosure - unless specific laboratory tests have been conducted to verify continued compliance with that particular equipment combination. Unfortunately, if no such evidence exists there is little that the security manager can do other than to be aware.

Only components carrying a CE mark should be fitted to intruder detection systems covered by this guidance.

Codes of Practice for alarm confirmation

In addition to the standards and regulations applicable to IDS, the UK has some Codes of Practice which may be of interest to the security manager. Reference to these is made here for information only.

If a response is required from a local police force, CNI sites should consult their CPNI adviser to check whether a local agreement exists which may override the requirements identified in BS 8243[13].

Codes of Practice take the form of guidance and recommendations; they are not intended to be used as specifications. Two documents of particular relevance are:

BS 8243[13] - Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – Code of practice

BS 8473[15] - Intruder and hold-up alarm systems – Management of false alarms – Code of practice

In response to unacceptably high numbers of false alarms placing a strain on police resources, the Association of Chief Police Officers introduced a policy[19] which places an increased emphasis on the use of alarm confirmation technology. Police response will be reduced or completely withdrawn if a system repeatedly generates false alarms.

When protecting critical national infrastructure, it may not be appropriate to wait for alarm confirmation before despatching the response force. However, the principle of verifying alarm events has proven to reduce the number of false calls. The security manager may find some of the methods described below useful when tackling sites that give persistent false alarms, and where the use of alarm confirmation techniques can be justified.

Whilst there are exceptions for installations protecting critical national infrastructure, as a general rule, to apply for police response or to have it reinstated, a security system must incorporate alarm confirmation technology.

The criteria for applying alarm confirmation are fully described in BS 8243[13]. Three types of alarm confirmation are described:

1. Sequential alarm confirmation

The IDS shall be designed such that a confirmed alarm is signalled in response to two separate alarm conditions from different detectors activated one after another within a time window of 30 to 60 minutes, the second alarm activation confirming that the first was not caused by a fault or spurious event.

As a rule of thumb, a single disturbance (e.g. a window blown open by the wind or perhaps a spider walking across the front of a motion detector) must not generate a confirmed alarm. Permitted sequential alarm combinations:

- 2 detectors of different technologies i.e. shock sensor & motion detector;
- 2 detectors of the same technology with non-overlapping areas;
- 2 dual technology motion detectors or 1 passive infrared and 1 dual technology movement detector. Their coverage may overlap but the detectors must be located a minimum of 2.5m distance apart;

- 1 alarm and 1 tamper signal received at the ARC;
- 1 SPT transmission path fault and 1 alarm or tamper;
- faults on 2 separate SPT transmission paths.

Sequential alarm confirmation with non-overlapping areas invariably leads to gaps in security protection.

During the un-setting procedure of IDS configured for entry/exit delays, all confirmation is delayed until after expiry of the entry time. Detectors that are activated during the entry time can be notified immediately by local audible warning device(s). After a further 30 seconds an unconfirmed alarm message is sent to the ARC regardless of how many detectors have been activated. Upon the expiry of the entry time a confirmed alarm message is despatched. Annex G of BS 8243[13] includes timing diagrams that explain the permitted sequences of alarm activations and alarm confirmation.

If at the end of the 30-60 minute confirmation time window a second activation is not received, the IDS should be reinstated so that again if one detector activates, an unconfirmed alarm occurs and the confirmation time starts.

2. Audio confirmation

Where audio confirmation is used, an unconfirmed alarm will open up an audio link at the ARC so that operators can listen for activity within the supervised premises to determine if the alarm is genuine and a response force despatched where appropriate.

The use of audio confirmation techniques requires the ARC operator to determine if an intrusion is in progress, often by listening to and trying to interpret a series of abstract noises. This method of alarm confirmation carries a higher risk of calling the police too often, or not calling the police when an intrusion occurs.

3. Visual confirmation

With visual confirmation, an unconfirmed alarm will establish a CCTV path so an operator at the ARC can view key areas in and/or around the supervised premises, to determine if the alarm is genuine and despatch a response force if necessary.

Audio or visual confirmation systems could be used in conjunction with sequential confirmation.

Methods of un-setting the IDS to meet the requirements of the ACPO policy

Further to the measures suggested for minimising false alarms from disturbances within the service environment, BS 8243[13] also provides methods to reduce the possibility of the IDS users accidently triggering unwanted alarms during the setting and un-setting procedures.

Five methods of un-setting the IDS are offered. Unless special concession for an installation has been granted at least one method is required to be eligible for a police response. If this requirement is necessary, for security purposes CPNI recommends the use of method number five.

1. The IDS is un-set before the user enters the supervised area/premises, by unlocking the designated entry door or by authentication at a token reader/ keypad. Forcing open the designated entry door should not unset the IDS, nor generate a confirmed alarm, nor disable alarm confirmation.

2. Unlocking the designated entry door disables all alarm confirmation. Alternatively, disabling alarm confirmation permits the designated entry door to be unlocked. The user then completes the un-setting procedure from within the supervised area/premises. Forcing open the designated entry door should not unset the IDS, or generate a confirmed alarm, or disable alarm confirmation.

⚠ Caution is advised when using this method of un-setting, as it permits the user to stray from the designated entry route, possibly triggering detectors and thereby creating false alarms.

3. Forcible entry cannot generate a confirmed alarm; this method is not acceptable for IDS covered by this guide.

4. The IDS is unset using a digital key, e.g. a radio key (or wireless fob) prior to entering the supervised area/premises or by electronic token, e.g. proximity fob from within the supervised area/premises.

⚠ Use of radio keys to unset the IDS from outside the supervised area/premises without first initiating the entry procedure is not advised since it opens up the risk of exploitation.

Radio Frequency Identification (RFID) tokens commonly used for the management of alarm systems transmit their ID in binary form without encryption and can be easily cloned. Many commonly available tokens can also be made to transmit their contents without the need of specialised equipment.

5. Un-setting of the IDS carried out in conjunction with the Alarm Receiving Centre. This method requires indication at the supervised area/premises that the un-setting procedure has taken place successfully.

It is likely that the BS 8243[13] Code of Practice will be superseded in future by the European standard prEN 50131-9 Alarm systems - Intrusion and hold-up systems Part 9: Alarm verification - Methods and principles[16] although the concepts are expected to be similar.

Intrusion detection: components

The IDS will comprise one or more of the components described in the following paragraphs. At the time of writing, IDS components have discrete functions, however in the future it is expected that the functions may be distributed among any of the IDS components or even integrated into other items of the building infrastructure. Detectors, for example, may in future perform some of the processing functions normally associated with control and indicating equipment (CIE).

Control and indicating equipment

Control panel

Typically, CIE will comprise control equipment (including the processing circuitry) housed within a robust enclosure (control panel) and at least one user interface (e.g. keypad/token reader with a display).

The main processing functions of the IDS are normally performed by the control panel, for example connections are provided to send and receive signals to and from the user interfaces to determine if the system is to be set or unset and to send status information to displays to inform the users.

Control equipment for commercial/industrial use tends to have quite a high level of processing power/capability and can incorporate all manner of configurable settings and options programmable by the installation engineer.

In addition to the internal tamper detection devices that signal when the cover is removed, this particular control panel enclosure has tabs to facilitate the fitting of tamper evident seals.

Care is required when selecting a control panel to ensure that its method of operation is convenient for the users and is generally compatible with the activities undertaken at the supervised premises. It is necessary to check whether the programmable options available can actually fulfil the specific needs of the application. It is not uncommon to find that awkward workarounds have been implemented within an IDS because shortcomings in the control panel operation have not been discovered until late into the commissioning or handover stages.

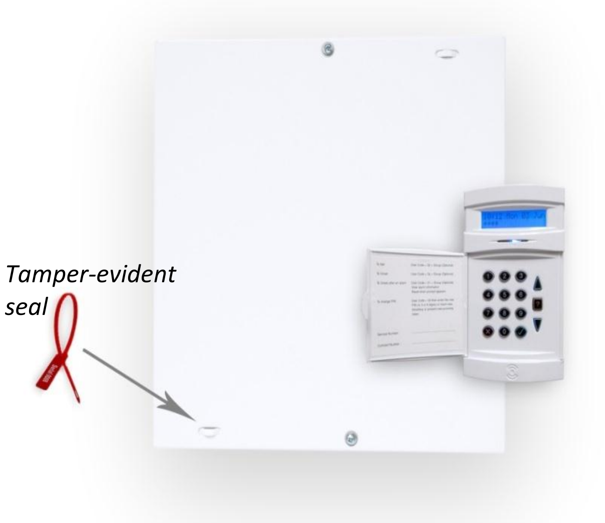


Figure 3: Example control panel with remote keypad/ display

Control panel enclosures are generally constructed from mild steel or ABS plastic. The use of mild steel is preferred since it offers better resistance to physical attack.

Tamper detection devices should be fitted in such a way that they detect both the opening of the control panel enclosure and the removal of the enclosure from its mounting surface.

Early versions of the EN standards did not require all IDS control panels be fitted with the capability to detect removal from the mounting surface and therefore not all control panels on the market have rear tamper devices fitted. Optional tamper detection kits may need to be purchased.

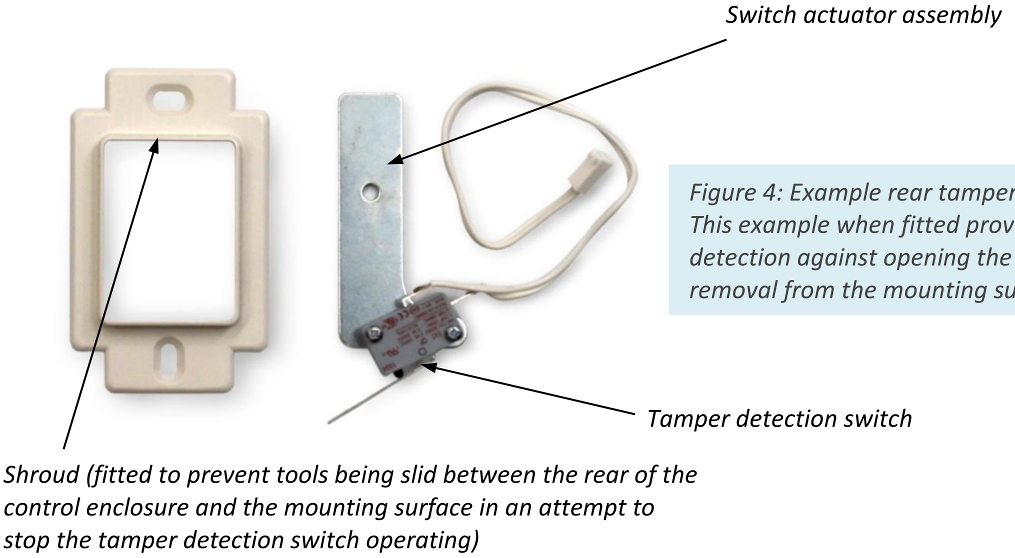

Switch actuator assembly
Tamper detection switch
Shroud (fitted to prevent tools being slid between the rear of the control enclosure and the mounting surface in an attempt to stop the tamper detection switch operating)

Figure 4: Example rear tamper detection kit. This example when fitted provides tamper detection against opening the enclosure and its removal from the mounting surface.

To avoid the risk of invalidating compliance with the EMC Directive and therefore the CE conformity of the IDS equipment, the use of optional tamper detection kits produced by the same manufacturer as the IDS equipment is recommended.

In general it is recommended that the manufacturer's instructions are followed when fitting the rear tamper detection devices to ensure they are not left vulnerable to compromise attack, e.g. by sliding objects between the wall and the rear of the control panel enclosure to prevent the rear tamper detection device operating.

In reality it may be impractical to expect the removal of the entire control panel from its mounting to go unnoticed, but prising the control panel enclosure away from the mounting surface sufficiently to expose large holes/access points intended for cable entry, may facilitate the defeat of the front cover tamper detection device, permitting the control panel to be opened without detection. Once inside the control panel the operation of the IDS can be completely compromised.

Where security is paramount, thought should be given to the possibility of other types of 'insider' attacks which may necessitate custom modifications to standard, off-the-shelf tamper detection mechanisms.

Inputs/outputs

Input circuits for detectors enable the control equipment to respond to intrusion events and outputs connected to alarm transmission equipment and/or warning devices raise the alarm.

Some CIE can be expanded with the connection of additional modules to increase system capacity if more input and/or output circuits are required.

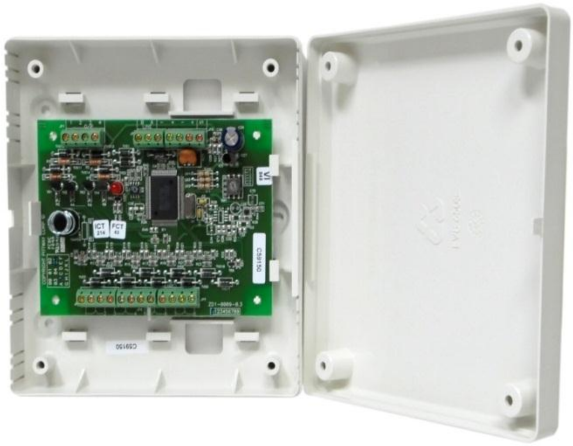


Figure 5: Typical input/output circuit expander module

Configuration

Configuration of the CIE is undertaken by the installer/commissioning engineer but the options chosen will to a large extent be determined by the needs of the specific application as identified from the completion of the OR.

Subject to the particular model of CIE deployed, some combinations of programmable option may invalidate compliance with the IDS standards (both the EN and/or CPNI standards). When the CIE has been selected from the Catalogue of Security Equipment[4] specific advice can be sought from CPNI.

Event recording

Where it is necessary to maintain records of activity associated with the IDS, CIE incorporating an event log will be required. Most CIE have this feature but the size of the event storage capacity varies between make and model. Normally the event log is a non-volatile memory (i.e. memory contents are retained even in the event of a total power failure) whose capacity is expressed in megabytes, e.g. 256mb, 512mb, 1024mb, or the number of events held. Some event logs are expandable by adding further memory chips.

Selection of the memory capacity will depend on the number of system users and the type of events to be recorded. An IDS incorporating access control type features that monitor people moving in and around the supervised premises will fill the event log a lot quicker than a similar system recording only set/unset events. Memory selection may also depend on whether remote back-up features exist. A remote back-up can automatically copy the contents of the event log to a larger storage medium, either in real time or at periodic intervals.

CPNI-graded IDS installations require event logs for audit and investigation purposes, i.e. who unset the system and when.

To ensure audits are robust, users should be individually identified, e.g. assigned unique tokens, PINs and/or passwords. The users' ID should determine their access rights to system menu options.

Remote access

Remote download / upload facilities offer convenient functions such as seamless updating of the IDS operating firmware and remote servicing, where the installation company can interrogate the IDS components for faults or impending faults without the need to actually visit site.

Such remote access into the IDS may not be desirable or compatible with the security level.

The use of remote access for CPNI-graded installations is discouraged. Isolating the IDS from external connections to remotes sites maximises security and reduces the risk of attacks. For CPNI-graded systems which run over information technology networks refer to CPNI's *Physical Security over Information Technology Guidance*[3] document.

Optional software applications permit remote/central management of the IDS. This can be a useful feature, for example, where site security is controlled/monitored by a team of security personnel. These management systems may also be integrated with other services such as the CCTV surveillance and building management controls. Any integration should be made with reference to CPNI's Guidance Document *Integrated Electronic Security Measures*.

Software applications normally run on standalone computers/servers and communicate with the IDS control and indicating equipment via Ethernet or serial links such as RS 485, using proprietary or IP based protocols. The level of security, i.e. encoding/encryption scheme, varies but unless CESG-approved its security is unknown.

User interface

Various types of user interface are available for setting/un-setting the IDS and/or accessing user menus. These include numeric/alphanumeric keypad, contact and non-contact token (e.g. proximity token/reader), swipe card, radio-based key, mechanical key, biometric reader and combinations of the above.

Selection depends on the security requirements associated with the IDS, user preference and compatibility with the particular CIE used. All IDS for critical national infrastructure use must use a PIN and/or password. A secondary means of verification such as a proximity token may be used in addition to a PIN and/or password.

Some CIE will have the user interface built into the control panel enclosure, however the use of separate user interface and control panel is recommended so that the control electronics can be located out of sight and in particular, away from the predefined entry route into the supervised premises/area, thus avoiding the attention of the intruder.

Most CIE provide the user with menu selectable functions to facilitate testing the IDS, for example a detector test function. Generally, the detector test functions place the CIE in a mode that allows a 'master user', e.g. the security manager, to confirm that all the detectors are functioning and reporting back to the control panel correctly. The security manager is advised to become familiar with such features and incorporate them in the audit routine/ confidence checking. Refer to the *Confidence checking* section for specific advice.

All components of the CIE must be located within the area(s) supervised by the IDS.

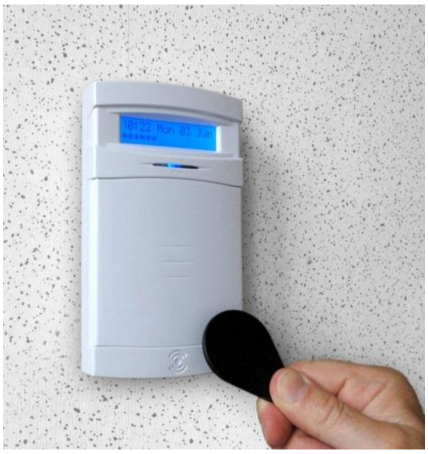


Figure 6: Example proximity token and reader

Power supplies

Power supplies provide a continuous electrical supply to all components of the IDS, (nominally 12V dc). Normally the primary power will be derived from the 220/240V ac mains supply. Components are incorporated within the power supply circuitry to protect against harmful voltage surges and other types of electrical interference that might cause the IDS to malfunction or in extreme cases become permanently damaged.

Generally, the control panel will incorporate a power supply unit to deliver electrical power to the control panel circuitry and a limited number of accessories such as one or more keypads. The capacity of the power supply unit and the total power consumption of the system determines how many accessories can be connected.

It is good practice to remove decals, logos and labelling if they remain visible after installation in case they can be used to identify the equipment make and model and/or the alarm company responsible.

In all but the smallest of installations additional standalone power supply units will be needed.

All IDS should incorporate a standby power source, such as a battery to ensure the system continues to operate in the event of a failure of the primary power source, e.g. during a power cut. Where no mains power is present, e.g. in a very remote location, IDS that operates from primary batteries or a generator can be used.

Selecting the correct power supply is essential since the operation of the IDS is wholly dependent upon the reliability of the power source to which it is connected. Until recently IDS power supplies were, more often than not, under rated and barely able to supply sufficient power to run the IDS properly.

The introduction of the European standard BS EN 50131-6[21] in 2008 effectively raised the performance level of IDS power supplies by introducing a recognised and consistent method by which the specifications claimed can be verified. In particular, compliance with the standard as demonstrated by third party testing, confirms that a supply can deliver maximum power to the IDS and still recharge the standby batteries correctly under the various climatic conditions that might be expected in the service environment. Correct charging of the standby batteries requires the automatic adjustment of the charge voltage in accordance with changes in ambient temperature.

The standby capacity must be specified according to the maximum expected duration that the IDS is required to function following the loss of primary supply, for example during a mains power outage.

Guidance for standby power durations are given for commercial IDS in Clause 9.2 of BS EN 50131-1, typically 60 hours for an EN security grade 3 IDS fitted with a 'Type A' power supply. For the purposes of the UK PD 6662 scheme the stated standby duration has been reduced to 24 hours and can be further halved to 12 hours when a prime power source fault is notified to an alarm receiving centre.

The charging circuitry is required to recharge a discharged standby battery to 80% of its stated maximum capacity within 24 hours.

The majority of non-wireless type IDS use sealed lead acid gel type batteries which have a final discharge voltage, typically 10.5V for a nominal 12V battery. If the voltage at the battery terminals falls below the final discharge voltage, the battery must be replaced because its capacity to store charge will be significantly reduced.

It is worth noting that the desired standby duration can only be achieved where supply of the primary mains power is regular with only occasional power outages. Frequent power outages are likely to prevent the standby battery from re-charging sufficiently and therefore must be avoided.

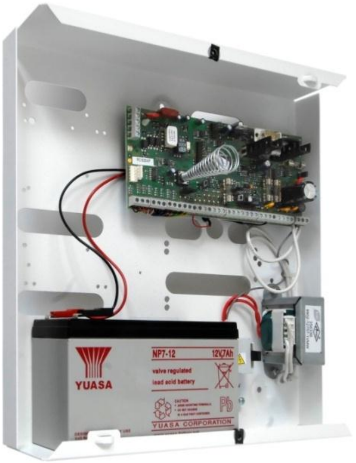


Figure 7: A control panel with cover removed exposing the control circuitry, mains step down transformer and standby battery

Caution: when specifying a power supply, ensure before installation that its specification can adequately fulfil the power requirements of the IDS.

Good practice requires that compliance with the BS EN 50131-6[21] standard be demonstrated where possible, e.g. by the presentation of a third party approval certificate and/or a test report. This will also confirm that the power supply has been independently assessed to verify that it is electrically safe.

Further information about supplies can be found in BS EN 50131-6[21], but in summary three types of power supply are described:

Type A: The primary power source is mains power. In case of mains failure, a rechargeable battery powers the IDS. Under normal conditions no power is drawn from the battery but it is automatically kept charged from the mains supply. Alternatively, in addition to the mains power source a standby generator may be provided to further increase resilience.

Typically the batteries of type A power supplies will be of sealed lead acid gel, nickel cadmium or more recently, lithium ion technology. Each type, whilst capable of providing a number of years' service, will need to be replaced after approximately 3-5 years.

Type B: Power supplies are less commonly used than type A. The primary power source is mains power and in case of mains failure a non-rechargeable battery such as a lithium cell, powers the IDS. In addition to the mains power source a standby generator may be provided to further increase resilience. The maintenance procedure associated with type B power supplies shall include defined time intervals when the non-rechargeable battery must be replaced.

Type C: The electrical power to the IDS is supplied by a non-rechargeable battery such as a lithium cell. No mains or standby generator is present. An example of the use of a type C power supply is a battery powered wireless detector (note: wireless IDS are not recommended and can only be used at CPNI Protection Level BASE). The maintenance procedure associated with type C power supplies shall include defined time intervals when the battery must be replaced.

Generally, type A power supplies will be used to supply wired CIE and ACE.

The power units will be located either within the control panel enclosure or within a separate standalone enclosure. A typical IDS installation will often have both.

Standalone (remote) power supplies are particularly useful where additional power units are required, either to supplement the control panel power supply or where equipment is located remote from the main IDS components. In any event standalone power supply enclosures are expected to fulfil the same tamper protection requirements as those of the corresponding control panel to match the designated security grading of the installation.

The provision of power supplies should be solely for the use of the IDS.

It is good practice to specify the power and standby capacity of IDS power supplies with a safety margin to ensure the desired specifications can be met under all conditions.

If future expansion of the IDS is anticipated it may be cost effective to install higher rated power supplies and standby capacity from the outset. However, it should be noted that higher battery capacities generally means increased physical size which in turn may require a larger enclosure thereby significantly increasing costs.

Electrical connection to the mains supply shall be via an un-switched fused spur point in accordance with the electrical installation regulations of BS 7671[17].

Power supply faults (including mains power outages) shall be recorded in the IDS event log and indicated at the user displays when the system is unset. No indication of a power supply fault should be displayed when the IDS is set. Power supply faults must also be notified to the ARC, although notification of mains power outages may be delayed for a maximum of one hour.

Detectors

Detectors provide the sensory parts of the IDS enabling the presence of intruders to be detected. They are placed in and around the supervised premises/area in strategic locations, sometimes connected in groups in order to form detection zones and areas.

The operation of each detector should be monitored individually by the control panel but there are exceptions. The exceptions are protective switches monitoring a door, where each leaf of a double door is monitored by individual switches connected together, and vibration detectors monitoring the same contiguous area where up to five devices may be monitored together.

There are two principal detection implementations, perimeter detection and trap detection. Some detection technologies may span both, an array of active infrared beams for example.

Perimeter detection

Detectors installed to detect entry or attempted entry through the external boundary of the supervised premises/area such as the walls, roof, doors or windows. The detectors should be positioned to detect a forcible attack at the most likely points of entry. Typical perimeter detection device types are:

- Protective switches
- Glass break detectors
- Vibration/shock detectors
- Active infrared detectors

Trap detection

Detectors installed to detect intruders moving within the boundary of the supervised premises/area.

- Motion detectors e.g. passive infrared (PIR), microwave and dual technology detectors
- Active infrared detectors
- Protective switches
- Capacitive detectors
- Inductance detectors
- Acoustic detectors

Unless the area to be protected is particularly benign (e.g. museum display case), the use of capacitive, inductance and acoustic detectors is not recommended as minor disturbances with their environment can result in unwanted alarms. The correct positioning and adjustment of detectors is essential in order to achieve optimal detection performance with a high tolerance to false alarms.

⚠ Motion detectors used in IDS installations at CPNI Protection Level ENHANCED and HIGH, and all Class Ratings must have the masking detection function enabled.

Further information about detectors and detection technology can be found in Annex A.

Warning devices

Warning devices for the notification of intruder alarm events may be a bell, siren or a visible indicator such as a high intensity strobe light. Their purpose is to attract attention to warn on-site personnel of an intrusion or attempted intrusion, or to scare away the intruders.

In most instances of CPNI-graded IDS installations, warning devices are not fitted; the automatic alarm transmission system being the only means of notification, and where the apprehension of the intruder is desirable.

It is possible to fit an automatic alarm transmission system and warning devices yet not alert the intruder following an alarm activation. This is achieved by delaying the operation of the warning devices, giving police time to reach the supervised premises.

Since warning devices are not generally fitted on CPNI-graded installations no warning devices are listed within the CSE.

Further information about warning devices and the different types available has been included for reference in Annex B.

Alarm transmission systems (ATS)

The primary means of signalling an alarm on a CPNI-graded installation is normally via an automatic alarm transmission system.

Signals or messages are sent from a transceiver (SPT) located in the supervised area/premises to an alarm receiving centre (ARC) where the decision is made to alert the appropriate key holder or to promptly dispatch a response force. The alarm receiving centre may be situated on site (e.g. a guard room) or at some other location remote from the protected site. The objective of the ATS is to transmit the alarm message as quickly and securely as possible.

Various transmission media exist and it is for the system specifier to select the most appropriate. Some popular examples are listed below:

- **PSTN**: (Public Switched Telephone Network): alarm messages are sent via conventional copper wire telephone lines (e.g. BT Redcare 'Classic' SPT). Consideration must be given to other communication equipment that may share the same telephone connection. The use of an ex-directory 'Incoming Calls Barred' (ICCB) telephone line dedicated to ATS use is recommended. Where necessary a 'Leased Line' can be purchased that will limit the use of the line solely for the transmission of alarm and fault monitoring messages. PSTN technology has proved itself reliable in the past but the equipment designed for use with the traditional copper based networks is time limited as the network infrastructure migrates over to optic fibre.

- **ADSL Broadband** (Asymmetric Digital Subscriber Line): a data communications technology that enables fast data transmission over copper telephone lines and with a suitable interface, optical-fibre. Messages from SPTs fitted with one or more Ethernet ports are sent using Internet Protocols (IP) typically using TPC/IP or UDP, which have the advantage of fast transmission times. The speed is dependent upon the number of network nodes through which the message must travel but transmission times of less than 3 seconds to traverse the UK are not uncommon.

Concerns exist about the control and maintenance of network equipment such as routers and switches through which the alarm messages must pass. Many routers, for example, do not have uninterruptible power supplies, therefore if the mains power fails, the alarm transmission path is effectively lost. If dual path transmission is used, there will at least be a notification sent to the alarm receiving centre (ARC) indicating that mains power and the primary transmission path have been lost. To avoid loss of power routers can be provided with an uninterruptible power supply, these must be specified at the design stage.

- **GSM (Global System for Mobile communications)**: offers a wireless link using radio from the supervised premises/area to a base station remotely located. Usually there will be a landline connection from the base station that takes the message through the conventional transmission networks such as BT's and on to the alarm receiving centre. Some models of SPT make use of GPRS, the General Packet Radio Service over GSM as it offers competitive running costs.

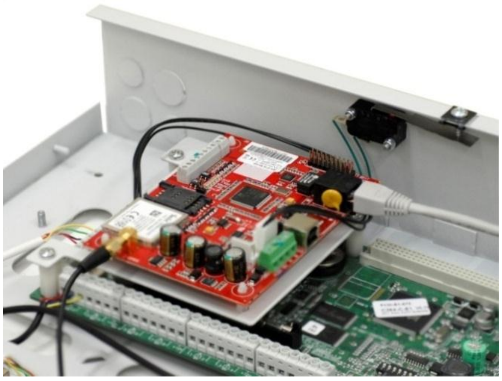
  For installations graded at CPNI Protection Levels ENHANCED and HIGH and all CPNI Class Ratings alarm transmission equipment operating over GSM for the primary communications link is not recommend.

- **VHF (Very High Frequency) communication**: a radio-based method often deployed for point-to-point communication, for example, one or more supervised premises transmitting direct to an on-site guarding station. There are also other types of proprietary radio-based systems in which each of the installed supervised premises transceivers link together to provide a network (or mesh) of transmission paths for increased resilience. However the effectiveness of such systems relies upon there being sufficient numbers of SPTs within operating range to form a robust network.

  Radio-based alarm transmission equipment is not recommend for use as the primary communications link for installations graded at CPNI Protection Levels ENAHNCED and HIGH and all Class Ratings.

- **Direct line communication**: perhaps the most appropriate for the transmission of alarm and fault monitoring of high security IDS. It comprises a specific hardwired monitored interconnection between the supervised premises transceiver and the alarm receiving centre across which coded/encrypted data is sent.

  Subject to geographic location and the particular operating requirements, direct line communication may unfortunately be the most expensive of the options available.



Many supervised premises transceivers comprise a PCB module intended for fitting inside the enclosure of a control panel or auxiliary power supply.

Figure 8: a dual transmission path (Ethernet/GSM) supervised premises transceiver (in red) mounted inside a control panel.

Selection of the transmission media is dependent on a number of factors including initial connection fees, operating costs, availability and the level of security integrity required. The selection may also be determined by the preference to use a specific SPT or network provider.

Products available offer single or multiple transmission path solutions, dual transmission path being the most common for protecting high risk applications. An example of dual transmission path SPT is an Ethernet-based primary transmission path for use over ADSL broadband with a back-up GPRS-based secondary transmission path to provide a level of resilience should the primary path be lost.

As a minimum, SPT required for applications conforming to Protection Levels BASE, ENHANCED, HIGH and Class Ratings 1 to 3 shall incorporate the means to verify that the alarm transmission networks are available and shall report a fault condition to the alarm receiving centre within the times shown in Table 2.

Table 2: Fault reporting requirements

Parameter	**Protection Level**			**Class Rating**		
	BASE	ENHANCED	HIGH	1	2	3
Fault reporting time	10 minutes	180 seconds	20 seconds	180 seconds	180 seconds	20 seconds

⚠ It is recommended that polling or an equivalent method of supervision be used to confirm availability and correct operation of the primary path between the supervised premises transceiver (SPT) and the receiving centre transceiver (RCT).

The secondary path should also be monitored, either by polling or by background checking to confirm that an operational communication channel exists between the supervised premises transceiver (SPT) and the receiving centre transceiver (RCT).

The alarm transmission system (ATS) performance parameters of the secondary path should match those of the primary path (e.g. with respect to alarm transmission timing and the security integrity of the transmission path) except that, during times when the primary path is functioning correctly, the polling or background checking of the secondary path may generate a fault report at a reporting time interval greater than that associated with the designated primary path.

In the event of failure of the primary path, the checking of the secondary path should step up to at least equal the performance of the claimed ATS rating of the primary path.

The 'stepped up' reporting time should persist until the fault is cleared, after which the reporting function is permitted to return to normal.

⚠ It is normal practice for alarm transmission system providers to operate 'stepped up' reporting for limited time (typically between 24 and 96hrs), regardless of whether the failure of the primary path has been rectified. Security managers are advised to obtain written confirmation from the alarm company that ‘stepped up' reporting will persist until the fault is cleared.

Wherever possible, the alarm receiving centre (ARC) monitoring equipment shall be duplicated to provide resilience should a single item of monitoring equipment fail or the ARC itself become the subject of an attack.

As well as transmitting alarm messages the functionality of many alarm transmission systems has been extended to provide additional features such as remote diagnostics and remote servicing of the IDS system. Provided the IDS components incorporate the means to monitor and report faults or pending faults, the SPT is able to call a service engineer before the user becomes aware that the IDS has developed a fault. The ARC or the installer can also inspect CIE event logs and/or update the system firmware without having to attend site.

Clearly this type of functionality can have significant operational advantages and cost savings. Such features should be made available in line with CPNI's *Physical Security over Information Technology Guidance*. The ability to access the IDS remotely and change the firmware and/or alter site configuration data could place at risk the security integrity of the entire system and is not recommended.

Where appropriate, i.e. as determined by the CPNI grading, upload / download facilities should be disabled, preferably in hardware so that there is no physical means for the CIE to connect to the publically accessible transmission networks outside the supervised area / premises.

Intrusion detection: systems

Commissioning

Upon completion of the installation a full inspection of the IDS should be carried out by the alarm company to confirm that it has been installed in accordance with the system design proposal. The inspection shall include a check of the following items, where fitted:

- User interfaces
- Control panel
- Power supplies
- Expansion modules
- System interfaces
- Detectors
- Warning devices (internal and external)
- Supervised premises transceivers
- Interconnections and joint boxes
- Remote management console

Tests should be made to confirm that all the components are working correctly. A complete system test should also be carried out and witnessed by the site manager or the appropriate representative. The system test should include checks to confirm that all tamper detection devices have been fitted and that each functions correctly.

It shall be ensured that the supervised premises transceiver (SPT) sends the corresponding message (e.g. alarm, tamper, fault, open/close as appropriate) and that each message is correctly received and enunciated at the ARC within an acceptable time.

Note: This check is often done at a later date than the main installation because the lead time to process the ARC and police paperwork can often exceed the installation lead time. If that is the case the tests should be conducted by the commissioning engineer and preferably witnessed by the security manager or representative.

Disconnection of the transmission paths interconnections should also confirm that the corresponding transmission path loss is enunciated at the ARC within an acceptable time.

Note: where GSM is used as a back-up ATP for an alarm transmission system it may not be possible to entirely disconnect the radio path if the SPT is located within close proximity to a GSM base station.

The security manager shall check that any deviations from the system design proposal have been recorded in the 'as-fitted' documentation and that the location of all devices has been correctly documented. Refer to *Documentation and records* for further advice.

The detection performance of each detector should be tested and compared with the requirements included in the system design proposal. If necessary final adjustments should be made to the detectors by the alarm company (e.g. detection range, sensitivity or coverage).

Suggested methods of 'in-service' testing of motion detectors are provided in the section entitled *Confidence checking*.

At this stage it is recommended that the details of the detection performance test results (e.g. the position within the protected area where detection occurs) be recorded (see Figure 13), as this information is likely to be of use in future when confidence checks (also known as audit checks) of the IDS are made.

The configuration parameters of site specific data within the CIE should be checked to verify that the indications and notification outputs provided are as required by the system design proposal and installation plan.

Many commercial level CIEs will have the capability to provide a hard copy print out or CSV files of the system configuration parameters and site specific data. It is recommended that the security manager obtain copies of the print out or CSV files where possible to retain for future reference.

System handover

Upon handover of the IDS, a full demonstration of the system operation should be provided, including the operation of the CIE, each detector and where applicable, each hold-up device.

Advice shall be given by the alarm company explaining how and when these devices should be tested in future. There shall be confirmation that all required tamper detection devices have been fitted and operate as intended. It is not uncommon for back tamper detection devices to be fitted incorrectly or in some cases, not fitted at all. These checks must be conducted with the alarm company present as opening the IDS components should create a tamper condition that will require an engineer reset. After handover an engineer reset will incur a call out charge.

An explanation of the functions of the CIE, ACE and ATS should be provided along with written procedures for communicating with the ARC, emphasising what to do in the event of operator error creating a false alarm condition and the need to abort an alarm response.

Written operating instructions should be provided for the IDS, including explanations of how the CIE is operated including specific setting and un-setting procedures.

System users must be made aware not to obstruct the field of view of motion and active infrared detectors and given guidance how to avoid unwanted alarms, e.g. the closing and securing of windows and doors prior to setting the IDS.

It is important to allow sufficient time to conduct the hand over process properly so that the security manager can be satisfied the IDS has been installed to specification and is working correctly. There will be little defence for the security manager should it be later found, after a successful break-in, that an essential component was not actually fitted.

Prior to the final commissioning but subject to specific operational circumstances, it is recommended that the IDS be tested for an agreed period, typically 14 days, before going live. During this time the IDS shall have been free of false alarms. The IDS should be operated normally throughout the test but the ARC instructed to inform only the alarm company in the event of an alarm condition being reported.

Any abnormal events including alarms occurring during the test period should be investigated by the alarm company and corrective action taken. This process will also test the reliability and to some extent, the availability, of the ATS.

Following completion of the system test for the agreed period without unwanted activations or malfunction, the IDS should be fully commissioned.

Note: Special site requirements may obviate this requirement, but before dispensing with a system test, consultation should be made with police or other response force as applicable. IDS installed to the ACPO policy requirements should operate for 14 days without false alarms before the remote signalling is permitted to be used to call for police response.

Once the handover process is complete it is recommended that the security manager take detailed notes of detector performance and possibly photographs of the IDS components, their mounting locations and orientation.

Key performance parameters should be recorded, for example, how many beams of an active infrared detector must be simultaneously interrupted before an alarm condition is signalled.

These notes and photographs will provide an accurate record of the IDS at the time of installation and should be kept for future reference. Refer to the section *Confidence checks* for guidance on information that should be recorded.

Documentation and records

Documentation

Documentation should be prepared based upon the system design proposal but updated to reflect any changes to the actual IDS design found to be necessary during the installation process.

The as-fitted document should provide an accurate record of the installed system including details of the equipment fitted, its location, the types of cables used and their routing.

The security manager should keep safe a copy of the Operational Requirement (updated to reflect any changes made during the project) and the following documentation so that it can be made available should the IDS require modification, repair, maintenance, or audit. It is the responsibility of the security manager to ensure this documentation is kept up to date:

- The as-fitted document
- IDS operating instructions including any site specific instructions
- Installation company details and a 24hr contact method
- Service and repair company details if different from above
- Alarm receiving centre contact details (where applicable), and security password/codes required to abort the despatch of the response force in the event of a false alarm
- Details of any procedures relating to the verification of alarm conditions
- The name, address and telephone number of the key holder or organisation responsible for attending the supervised premises following a notified alarm condition
- Certificate of conformance*

**It is normal practice for the alarm company to provide the client with a certificate of conformance stating the IDS has been installed in compliance with the as-fitted document. Claims of compliance with any legislation, regulation(s), National or European Specifications should normally be included on the certificate of conformance.*

It is recommended that where appropriate, a master copy of any alarm monitoring or IDS management software installed on local computers/servers is retained by the security manager.

Accredited IDS installers will be required by their accreditation body (e.g. NSI or SSAIB) to provide the above information including their certificate of conformance, the amended detailed specification, as-fitted drawings and detailed test records, such as the voltage and impedance of every detection circuit. An on-site log-book shall be kept which records all service and maintenance visits.

The accreditation body has the right to inspect the system as part of their on-going audit process and can also offer a mediation service in the case of disputes regarding the installation, its servicing and maintenance.

Records

Detailed records should be kept of any alarm activations resulting either from genuine intrusion attempts or false alarms. Each entry should include the date and time of the event, the identity of the detector responsible for generating the alarm condition and in the case of a false alarm, the details of any remedial action initiated to prevent the occurrence of further false alarm conditions. Accredited IDS installers will have to maintain records of false alarms as part of their accreditation obligations.

The records should also include details of any modifications or additions to the IDS.

If required, records can be made available to persons responsible for maintaining the IDS but must be kept securely when not in use.

It can be useful to retain in escrow the engineer passwords/PINs required to configure the system. An arrangement can be made under contractual provisions between the alarm company and the IDS purchaser, whereby an independent trusted third party holds the password/PIN code information until the fulfilment of contractually-agreed conditions. This may prove difficult to achieve but can safeguard against rogue installers or those who cease to trade.

Maintenance

It is the responsibility of the security manager to ensure the IDS is properly maintained and promptly repaired when necessary. An arrangement should be made with the alarm company or other competent organisation for the maintenance and repair of the IDS.

To ensure the IDS continues to function correctly and reliably it should be periodically inspected and serviced. Equipment batteries will need to be replaced in accordance with the battery and equipment manufacturers' recommendations, and all IDS components will need to be tested and visually examined to confirm they have not suffered damage, their mountings remain securely fastened and that they are fully operational.

It is recommended that a maintenance schedule be agreed with the alarm company prior to, or immediately upon the completion of the installation.

Motion detectors may need to be cleaned both inside and out during maintenance visits. Despite measures to seal the optics of passive infrared motion detectors 'Thunder flies' are a common cause of false alarm when crawling across the pyroelectric sensor.

The following maintenance intervals are recommended:

Recommended Maintenance interval	**Protection Level**			**Class Rating**		
	BASE	ENHANCED	HIGH	1	2	3
	Yearly*****	6 monthly	3 monthly	6 monthly	6 monthly	3 monthly

Table 3: Recommended maintenance intervals
**IDS at Protection Level BASE with remote signalling, installed in accordance with the requirements of the ACPO Policy, will require maintenance at six monthly intervals.*

Where a SPT is fitted, arrangements must be made with the ARC to ensure testing does not result in the unwanted despatch of the response force, in particular when testing hold-up devices. Such arrangements are normally undertaken by the alarm company but with authorisation from the security manager. Third party approved commercial ARCs will have engineer authentication processes in place for this purpose, usually comprising name and password, but could be another form of ID and password or a coded phrase.

If warning devices are fitted, the occupants of the supervised premises should be informed about any test of the IDS which may result in the activation of the warning devices.

The security manager is advised to check if any parts of the IDS will be inoperable during servicing and if necessary implement alternative arrangements to ensure that the security integrity of the supervised premises/area is adequately maintained.

It is recommended that the system record/log book be checked by the security manager upon completion of the maintenance work to confirm that the details of inspections and repairs carried out during the maintenance visit have been entered.

Confidence checking

It is good practice to check the security integrity of the IDS components once a week* to confirm there has been no mechanical damage and that the components are still functioning correctly. It should also be confirmed that there have been no attempts to deliberately interfere or tamper with their operation. These confidence checks are sometimes referred to as audit checks.

** It is acknowledged that weekly checks of the entire system may not always be possible. It is therefore the responsibility of the security manager to produce a schedule appropriate for the specific application. Some factors which can influence the frequency of the confidence checks are: security level, type of IDS components, size of the IDS, and the activities undertaken at the supervised premises.*

In the event of the security manager becoming aware of damage or a fault on any part of the IDS the alarm company must be immediately informed so that the necessary remedial action can be promptly undertaken.

The following sections provide guidance for the confidence checks that are to be conducted on the specific parts of the IDS.

Control and indicating equipment

Visually inspect the enclosures of all user interfaces (e.g. keypads, digital keys/ token readers etc.), the control panel and any expander modules for evidence of tampering or mechanical damage.

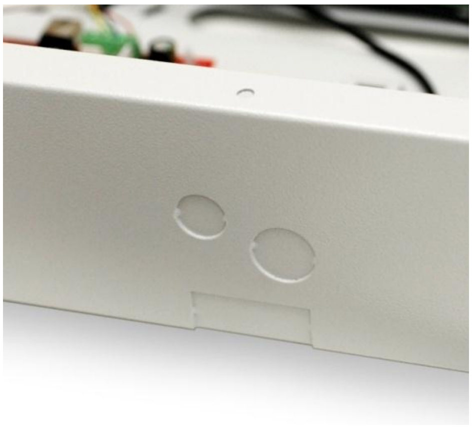


Figure 9: Unused cable entry/conduit knock-out points with blanking plates intact

Confirm that there are no unexplainable holes in the enclosures which may have been made for the purpose of attempting to compromise the tamper detection devices prior to the unauthorised opening of the enclosure(s). Check in particular unused cable entry points. All blanking plates and unused cable entry/conduit knock-out points should be intact.

Check all mountings/fixings are secure and enclosure covers held firmly in place.

Examine the event log(s) for unexplained events, fault messages and warnings. If wireless equipment is part of the IDS (e.g. at protection level BASE) check for low battery warning messages and other signal faults related to jamming or signal strength, which may have been caused by the alteration of the office space or furniture, for example.

Where keypads are fitted, check that the alphanumeric digits of the keypads corresponding with valid user codes cannot be readily identified by excess wear or finger marks on the keys. Clean the keys or arrange for replacements as appropriate.

Where swipe cards or digital keys/token readers are in use, confirm that there are no signs of tampering and that no foreign objects/components have been fitted. The internal inspection of the readers will need to be carried out in conjunction with the alarm company.

Detectors

Checks of detection performance should be made at regular intervals depending on the type of detector and the environment in which it is installed. It is recommended the checks be performed weekly where it is practical to do so.

Motion detectors

Motion detectors should be visually examined to confirm there is no physical damage, the fixings are secure and there are no signs of attempts to mask the detector.

Detectors should automatically warn if masking has been attempted and prevent the IDS from setting until the masking has been cleared and the masking message acknowledged. However, the detector should be closely examined for evidence of sprays, lacquer, paints or films having been applied to the front of the detector in an attempt to attenuate the transmission of infrared energy into the sensor.

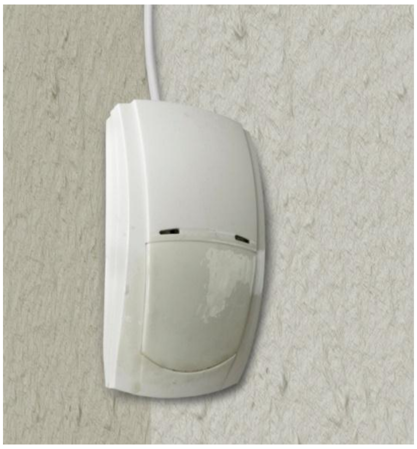


Figure 10: A Detector masked with paint. Examine the detector closely as the presence of some masking materials may not always be obvious.

Check for holes in the detector housing and replace any detectors which have damage or holes which would permit access to the interior.

For Class Ratings 2 and 3 tamper evident labels should be used that will clearly indicate if a housing has been opened.

Check the protected area for obstructions that might impair the detection coverage or the operation of the masking detection capability, possibly creating false masking conditions. A cabinet positioned too close to the front of the detector is an example.

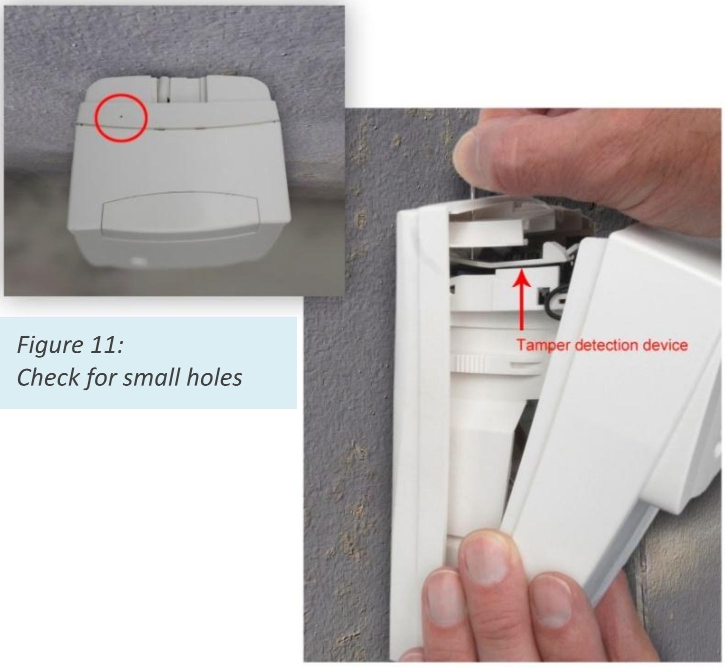


Figure 11:
Check for small holes

Regular walk tests should be performed to confirm that detection within the claimed coverage area results in an alarm condition being received at the CIE.

Most control panels have a 'walk test mode' accessible via a menu option. Entering the walk test mode will enable the local indicator on the detector to illuminate when detection has occurred. Some walk test mode options monitor and record the detector circuits that have entered into alarm during the walk test. This is a particularly useful feature when used with large IDS installations because it allows one person to perform a complete end to end verification check confirming that all the motion detectors fitted have successfully signalled an alarm condition back to the control panel.

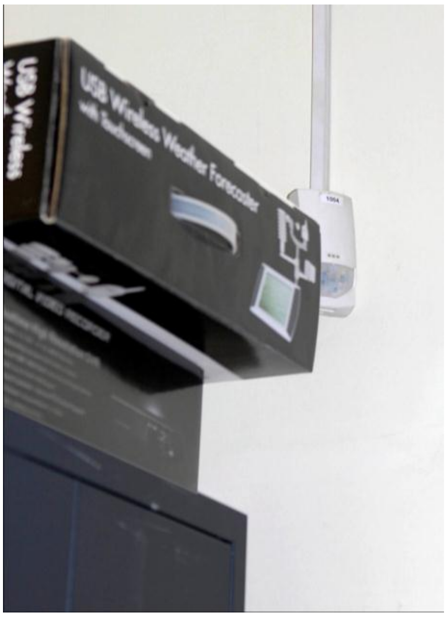


Figure 12: Check for obstructions

It is recommended that immediately after the system handover the security manager records the positions where detection occurs during a series walk tests performed in each of the protected areas.

The information recorded can be used to compare with the results of future walk tests to confirm that there is no deterioration of detection performance.

The method used to test the motion detectors may depend upon factors specific to the particular application, the position of fixtures and fixings for example. One method of testing motion detectors is suggested below:

Within the protected area, identify the most likely point(s) of entry for an intruder, noting that the direction and the distance moved may be restricted by the positions of furniture or stock.

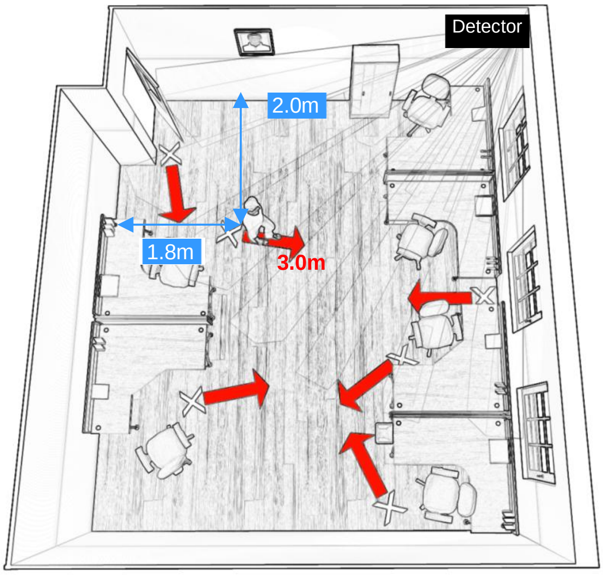


Figure 13: An example sketch identifying where in the protected area detection occurs

Starting from the point(s) chosen, walk upright with arms and hands by your side moving slowly (~0.2m/s) across the detection area until an alarm is signalled to the control panel or the walk test indicator on the detector has illuminated. Record the starting point and the distance moved, noting also your position relative to the detector at the time the alarm was created.

Once tests have been conducted at the likely points of entry, further points may be chosen to give confidence that a complete pattern of detection exits. If required the tests can be repeated at faster speeds.

It should not be possible to traverse a distance of more than 3.0m* across the detection area without generating an alarm condition. **The distance of 3.0m is specified within the EN standards applicable to motion detectors.*

The actual direction of the walk test and the maximum permitted distance that the intruder is allowed to move before an alarm is generated will depend upon the protection requirements specific to the application. If necessary the walk test procedure should be amended as appropriate.

The information and corresponding results recorded must be of sufficient accuracy to allow the tests to be repeated at any time with the expectation of obtaining similar results.

After comparison with the initial walk tests, e.g. those recorded immediately after the handover, if similar results are not achieved, check the following:

- Is the person performing the walk testing the same person that conducted the initial walk tests? Differences in body size and weight can have a significant effect on the detection performance.

- Are the clothes worn by the person performing the walk testing similar to those worn during the initial walk test? Loose fitting clothes or thick thermally insulating jackets may reduce the infrared emissions or lessen the microwave reflections and in the case of ultrasound, thicker clothing with absorb more of the ultrasound energy.

- Has the ambient temperature changed significantly? Detectors incorporating PIR technology are particularly sensitive to changes of ambient temperature. Generally the warmer the ambient temperature the less responsive the PIR detectors will appear.

- Has the interior of the protected area been changed? The addition or removal of stock, changes to furniture and the use of soft furnishings can contribute to perceived changes in detection performance.

If the reasons for the differences in the walk test results cannot be explained the alarm company must be consulted.

- ***Glass break detectors*** should be visually examined to confirm there is no physical damage and that their housings and associated cabling are securely fixed to the mounting positions. Check acoustic glass break detectors for signs of attempts to mask the detector by obstructing the microphone apertures in the detector housing.

Where junction boxes have been used to terminate interconnecting wires check their fixings and covers are securely fastened.

Windows that can be opened should be inspected to confirm they are not loose and the glass checked for chips and cracks that may result in false alarms. Arrange for immediate replacement if necessary.

Test the operation of each detector by using an appropriate test tool. Suitable test tools are usually available from the detector manufacturer. If no test tool is available it may be possible with some types of piezoelectric type glass break detector to create an alarm by tapping the glass sharply with a coin. (This method of test may not work with all types or models of glass break detector.)

Confirm that the alarm signal from each detector tested has reached the CIE and where present any local indicators have operated.

- ***Vibration/shock detectors***

Visually examine each detector/sensor to confirm that there is no physical damage and that they are securely fixed to their mounting substrate.

Where junction boxes have been used to terminate interconnecting wires check their fixings and that covers are securely fastened.

If vibration/shock detectors are used to protect doors and/or windows confirm the moveable parts of the door or window are not loose. Allowing them to rattle and create vibrations could eventually result in false alarms.

Test the operation of each detector by activating the remote test units if fitted, or by using a specific test tool supplied by the detector manufacturer. Alternatively if neither of the above are available, tap lightly on the vibration detector housing with a rigid implement such as a screwdriver.

Confirm that the alarm signal from each detector has reached the CIE and where present any local indicators have operated.

Vibration and shock detectors can be installed as arrays, i.e. up to five per array. This configuration is permitted by the standards provided each detector 'latches' after triggering to assist with any investigations to resolve unwanted alarms. Where such detectors are used they must be reset for new events to be reported. Resetting is normally an automatic function performed by the CIE when the IDS is next set. However, security managers are advised to confirm each vibration/shock detector can be reset following their 'weekly' tests.

- ***Protective switches***

To ensure reliable operation is maintained the protective switch, regardless of type, must be affixed to a stable surface. Frequent visual inspections of the protective switch fixings and checks for loose fitting doors and windows to which the switches are attached should ensure that potential problems are identified early. In particular check for worn hinges which allow the door to drop causing the misalignment of the magnet and the switch. Also, on roller shutter doors there is a common problem where older doors wear and then float laterally in their guide rails causing the magnet to mis-align with the switch by a very significant margin. Any indication of water staining on switches that are mounted on external doors must be investigated quickly and appropriate repairs to the building fabric made as soon as possible to prevent premature failure of these devices due to water ingress. Test the operation of each protective switch and confirm that the alarm signal has reached the CIE.

Active infrared detectors

Visually examine each AIR detector to confirm that there is no physical damage and that the equipment is securely fixed to its mountings. AIR detectors installed in high traffic areas such as warehouses where there is forklift truck movement, can often get damaged. Where this problem exists, consideration should be given to the physical protection of the detectors.

Confirm that the optical windows of the detectors are clean and free of dust. Arrange for cleaning of the optical windows with a soft cloth and soapy water if necessary.

Where junction boxes have been used to terminate interconnecting wires check their fixings and that covers are securely fastened.

Test the operation of each AIR detector by interrupting the infrared light beams as appropriate. Confirm that the alarm signal from each detector tested has reached the CIE and where fitted any local indicators have operated.

Warning devices

If fitted, warning devices mounted at height will be inaccessible when conducting a standard audit inspection; however the warning devices should be visually examined for physical damage, signs of deterioration or tampering. Look for things such as missing or loose cover screws or evidence of polyurethane foam injection. *(Expandable polyurethane foam may be injected into the warning device in an attempt to muffle the alarm when it is sounding.)*

Where possible confirm the warning device is securely affixed to its mountings. Visible warning devices should be free from dirt and dust so as not to reduce the intensity of the light emissions.

The operation of the warning devices should be tested. Testing can usually be performed by the selection of an appropriate menu option at the CIE.

Alarm transmission equipment

If the SPT is located in its own enclosure, confirm there are no signs of damage or evidence of tampering and that the equipment is securely affixed to its mounting.

Inspect the wiring to the site network equipment e.g. the network point, the router and switches etc., and if fitted, aerials and the associated cabling, confirm that they are in place and are undamaged.

Unless the ARC is local and within the control of the security manager, testing the alarm transmission equipment is best left to the alarm company. However, if the security requirements necessitate confidence checking of the alarm transmission system, an appropriate authentication procedure shall be agreed in advance between the ARC, the security manager and the alarm company.

Wiring and interconnections

Accessible IDS cabling shall be inspected for signs of damage and repairs arranged if necessary. The correct use of grommets and glands should prevent cables chaffing but these should be inspected periodically to confirm they remain intact.

Door loops, although designed to be flexible, can still degrade over time and with wear and tear.

System operation

The IDS can only be effective if used correctly and to a large extent this is achieved by good system design and adequate operator/user training. Thought shall have been given to the access levels attributed to the users of the IDS. The security manager for instance may need to assume a 'Master User' role responsible for changing local configuration settings and performing administrative procedures such as enrolling/deleting users. In contrast, general users might only be permitted to set and unset specific parts of the IDS.

Examples of the access levels attributed to the various types of user are provided in Clause 8.3 of BS EN 50131-1[10]. In summary these are as follows:

Level 1: Access by any person. Functions required to be accessible at level 1 shall have no restriction on access.

Level 2: User access, e.g. by an operator. Functions affecting the operational status (without changing an I&HAS configuration, e.g. site specific data). Access to functions required to be accessible at level 2 shall be restricted by means of a key or code operated switch or lock or other equivalent means. Level 2 key or codes shall not provide access at level 3 or level 4.

Level 3: User access, e.g. by alarm company personnel. All functions affecting an I&HAS configuration (without changing equipment design). Access to functions required to be accessible at level 3 shall be restricted by means of a key or code operated switch or lock or other equivalent means. Level 3 key or codes shall not provide access at level 4.

Level 4: User access, e.g. by the manufacturer of the equipment. Access to components in order to change equipment design. Access to functions required to be accessible at level 4 shall be restricted by means of a key or code operated switch or lock or other equivalent means.

A well-designed IDS should fulfil the primary security requirements with the least possible disruption to the legitimate occupants/users of the supervised area/premises. Inevitably there is a direct relationship between the security level and user convenience. Generally the higher the security level, the more intrusive the operation of the IDS becomes to the occupants but usually an acceptable compromise can be reached.

The correct choice of user interface is essential, for it is with the interface, i.e. the keypads, token readers and displays etc., that the system users will interact, particularly those required to set and unset the IDS on a regular basis.

Select the method of setting and un-setting most suitable for the prevailing local conditions. The technology used is largely a matter of choice provided the primary security requirements are addressed.

Other factors such as, the provisions of the Equality Act[25] must be considered. In some circumstances the requirements of the BS 8243[13] code of practice may also apply.

Setting the IDS

Setting can be achieved by initiating the procedure at the user interface of the CIE and then either:

- presenting a token to a reader located outside the supervised area/premises;
- pressing a 'final exit' button located outside the supervised area/premises;
- throwing a contacted lock installed in the final exit door;
- operating a protective switch fitted to the final exit door.

Where remote signalling capability exists, the setting of the IDS can be performed by the ARC in conjunction with the system user. This is the CPNI-recommended procedure for setting the IDS.

Un-setting the IDS

As a basic principle it is recommended that users are physically prevented from entering the supervised premises whilst the IDS is set. This means providing a physical barrier that has an electrical connection to the IDS, such as a shunt lock. Unlocking initiates a timed un-setting procedure which is completed by the entry of a PIN code at a keypad and, if secondary authentication is required, the presentation of a token at a reader inside the supervised premises. It is however acknowledged that circumstances within the specific application may mean that this configuration is not possible.

The following types of user interface technologies are available; PIN codes/keypads, swipe cards, mechanical and electronic keys/tokens and bio-metric readers. The use of wireless fobs is only permitted at Protection Level BASE.

In most cases it should be possible to obtain a method of setting/un-setting that is simple to use and best suited for the application. However, despite the complexity and the numerous configuration options of modern CIE sometimes the preferred solution cannot be provided by a particular make/model of CIE. It is therefore advisable to seek proposals from multiple providers and select those that can offer the solutions required.

Where access to the supervised area/premises is under time control and the un-setting of the IDS is time restricted accordingly, detailed access schedules must be established so that they may be used to correctly programme the CIE configuration data. In addition, assurance must be obtained confirming the ability of the ARC to handle such time schedules correctly.

The IDS may also be able to perform functions other than intruder detection. It may control lighting, e.g. switching off lights in unoccupied areas to conserve energy usage. Whatever additional features are provided their implementation must not impede primary functions of the IDS and its ability to detect and notify the presence of intruders. Reference should be made to CPNI's guidance document *Integrating Electronic Security Systems* before an integration is specified.

Alarm handling

The security manager must ensure that a procedure is drawn up clearly defining how notified alarms are to be handled and what actions must be taken and by whom. Those responsible for implementing the procedure must be properly instructed and made aware of their duties.

The procedure shall take account of system functionality, the security level, the perceived threat(s), and any other prevailing factors. It shall at least consider the following in the event of an alarm:

- Who needs to be notified, how and when and what their responsibilities are
- The type of response required
- What subsequent actions are required
- A back-up plan should the preferred options not be available

The alarm company may be required to check the operation of the IDS where a genuine alarm has been determined, this will demonstrate the system is functioning correctly and confirm that no deliberate interference or tampering with the IDS components has occurred. In any event the operation of all detection devices should be tested before the IDS is next set. Refer to the section on *Confidence checking* for further advice on testing detectors.

Management of false alarms

The alarm company should have in place a documented process by which the occurrence of false alarms and unconfirmed alarms is identified. The process should include a means by which any installation giving more than an acceptable level of false alarm is identified and reported to the appropriate levels of management for information and action.

In the event that an alarm is established as false, the cause, if known, must be documented and corrective action taken to prevent recurrence. Such action may necessitate a service visit by the alarm company, particularly if the cause of alarm is not identified as all unexplained alarms must be investigated.

Users of the IDS shall ensure their actions do not contribute to the false alarm statistics, failure to do so can be inconvenient and costly.

As a general guide adherence to the following is recommended:

- Ensure the IDS is only operated by users that have undergone training and fully understand how to use the IDS correctly;
- Before leaving the premises ensure that all doors and windows are closed and securely fastened, walking around and visually inspecting the supervised area/premises is the only effective way of doing this;
- Where motion detectors are installed make sure the protected areas are kept free of moving objects. Particular attention should be paid to swinging signs and Christmas decorations. Electric fans, heating or ventilating systems should all be switched off if possible and animals and birds kept out of areas monitored by the IDS;
- Ensure that detection devices are not obstructed by stock or other items and make sure nothing is left that might fall or topple over when the IDS is set;
- Always use the prescribed exit/entry route procedure as agreed with the alarm company. Entry through any door other than the one designated should be physically prevented;

- If the supervised premises opening or closing times are monitored by an alarm receiving centre, ensure the ARC is notify of any variations from the agreed times;
- Consult the alarm company about changes to the building or its contents if the changes are likely to affect the performance of the IDS. Permit only the alarm company to make changes to the IDS and place the system on test when building alterations are taking place. Implement alternative protective measures where necessary; and
- Ensure that regular servicing and preventative maintenance of the IDS is undertaken.

Operator training

Adequate operator training is essential if the IDS is to be used correctly. Each user must as a minimum be given a basic understanding of how to set and unset the IDS and be made aware of the potential sources of false alarm and how to avoid them.

All users regardless of responsibility must undergo training, including those with limited access level permissions, such as a cleaner. Where possible the training should be conducted by competent personnel from the alarm company.

It is recommended that a competent person from the alarm company instructs the 'trainer' or members of the upper security management team before disseminating the information to other users of the IDS.

The training should at least include:

- The checks to be made prior to starting the setting procedure, e.g. that all doors and windows are closed etc
- The method of setting the IDS
- Interpreting display messages, indications and warnings
- How to abort the setting procedure
- What to do if the IDS will not set
- Reading and interpreting the contents of the event log (subject to the appropriate access level)
- The use of duress codes and/or hold-up devices
- How to unset the IDS
- What to do in the event of a notified alarm
- The secure contact procedure for communicating with the ARC

Written instructions for operating the IDS must be provided by the alarm company.

The security manager may wish to enhance these instructions or add instructions that are specific to the particular application. Subject to the type of activities performed at the site and the corresponding security level, additional procedures may be relevant. For example, the specific actions to be undertaken in the event of a genuine alarm occurrence such as an immediate inventory check for missing assets/ protectively marked material.

The site facilities personnel with the responsibility for the supervised area/premises must also be given appropriate training and be advised of the duties expected of them.

Records of each person trained shall be retained by the security manager.

Performance

Developing intrusion detection equipment capable of providing optimal detection performance whilst maintaining a high level of immunity to false alarms is a challenge. The equipment designer does not know the environment where the security equipment might be used, nor to what types of disturbance it might be exposed.

Invariably, the design will be a reasonable compromise of detection performance versus immunity. There is therefore an obligation on the part of the specifier, the alarm company and the end user(s) to help minimise the risk of false alarms and maintain an acceptable level of detection performance.

False alarms broadly fall into four categories:

- Alarms resulting from a malfunction of one or more IDS component;
- Alarms created by user error;

  Experience has shown that most false alarm events are caused by the IDS users. Either directly, by not following correct procedures when operating the system, or indirectly by ignoring the presence of potential false alarm hazards;
- Alarms created by the detection of a stimulus other than an intruder, e.g. a stack of boxes toppling over and triggering a motion detector;
- Alarms resulting from environmental disturbance; e.g. air draughts, heaters, air-conditioning, electrical interference etc.

With the introduction of automated manufacturing processes and the use of low power surface mount technology, the reliability of IDS equipment improved significantly and as such component failures in service are less frequent than they used to be.

The occurrence of false alarms due to disturbances within the service environment and those unintentionally generated by user error remain, but it is possible to actively manage the use of the IDS to limit the occurrence of false alarms to an acceptable level. Even well managed IDS will at some point create false alarms. The size of installation, the number of users and the quantity of the detection devices, all contribute to the probability of unwanted alarms.

The number of false alarms that can be tolerated may also vary with the particular application and the type of response force required to attend notified alarms. The attendance of an onsite guard force in the event of an unwanted alarm condition, for example, would perhaps not create a significant inconvenience. A police response to a false call is always undesirable.

As a guide to the number of false events that can be tolerated, reference is made to the ACPO policy[19]. The policy requires the immediate withdrawal of police response from IDS that has signalled 3 unwanted alarms within a rolling 12 month period per installation. Refer to Annex A for further information on avoiding false alarms.

Availability

The IDS and the associated alarm transmission system (ATS) should be expected to provide as a minimum, the reliability performance to achieve the following availability in any 12 month period:

Table 4: Minimum IDS and ATS availability

Availability	**Protection level**		
	BASE	ENHANCED	HIGH
IDS	99.5%	99.8%	99.8%
ATS	99.5%	99.8%	99.8%

Availability requirements for IDS and ATS should be specified within the tender documentation and be written into the contract with the alarm company.

IDS availability can be monitored by the security manager over a 12 month period. For example, IDS with an availability requirement of 99.8% should not be out of service for more than 17½ hours (approx.) throughout the year. Systems failing to meet the availability requirements should be reported to alarm company and corrective actions agreed.

It is acknowledged that the alarm company may not always be responsible for prolonged unavailability, for example if awaiting a replacement part.

If the OR demands greater availability, consideration could be given to the deployment of suitably trained resident maintenance personnel and stocks of spare parts held on site, thus reducing the time needed to procure replacements.

Availability of the ATS networks is equally as important, if the transmission networks have frequent or long periods of downtime due to faults or prolonged maintenance, the probability of an alarm message successfully reaching the alarm receiving centre within an acceptable time can be significantly reduced.

In some circumstances it may be possible by special agreement with the ARC and alarm company, to monitor ATS availability via the data stored from polling signals transmitted between the SPT and ARC. But this also requires the receiver software to have the necessary functionality and in most cases ATS availability can only be effectively monitored by those ATS service providers operating fully managed networks, a factor that may influence the choice of ATS used.

Integration

There is a growing trend towards integrating IDS with other types of system, such as access control, fire and emergency management, HVAC, lighting controls and communications services, even networking a variety of systems at locations remote from each other so they can communicate as if they were a single system. Distributed access control for example, can authenticate user credentials within seconds from the opposite side of the globe.

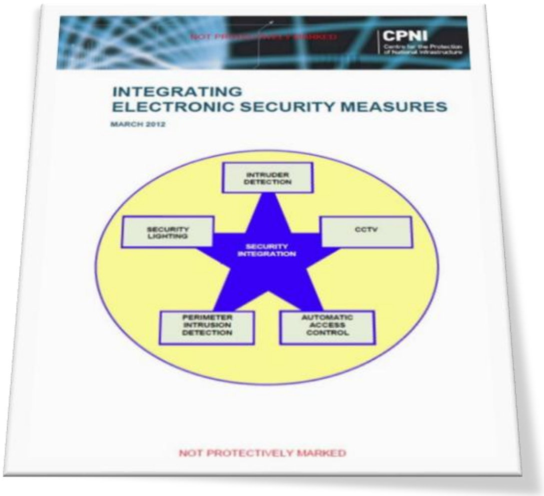
To date, the integration of IDS with other services tends to be via an optional interface electrically connected between the IDS control panel and a common communication BUS. The interface converts the signals from the IDS into a protocol recognised by other components sharing the BUS. To date there has been some reluctance by equipment manufacturers to fully integrate the IDS into a common building control platform, in part due to commercial strategy and also because of the difficulty in resolving conflicts between the relevant standards for the different equipment.

Whilst full systems integration can bring significant advantages (e.g. the use of less interconnecting cable, a single maintenance contract etc.), the advantages must be balanced with the possibility that a failure of a single part of the system might render the whole system non-functional. Service personnel must be adequately trained to maintain all parts of the integrated system to a high standard. Nonetheless the continuing trend is to integrate security systems with facility management and personnel operational procedures.

The integration of CPNI-graded IDS installations with building management systems (BMS) is discouraged as their management is usually undertaken by electrical engineers and not by security trained personnel. Connection to other non-security related services may create vulnerabilities that can be exploited by an attacker.

The deployment of IDS that can demonstrate compliance with DD CLC/TS 50398[23] is favoured as it confirms components of the system can function without interference from other connected services. To maintain the CPNI grading of an integrated system for all components, compliance with the applicable CPNI standards shall have been demonstrated by testing.

The decision to integrate IDS with automatic access control and other sub-systems must only be made after careful consideration of the possible implications. Please refer to CPNI's *Integrating electronic security measures*[24].



NOT PROTECTIVELY MARKED

CPNI
Centre for the Protection of National Infrastructure

INTEGRATING
ELECTRONIC SECURITY MEASURES

MARCH 2012

NOT PROTECTIVELY MARKED

Figure 14: Integrating electronic security measure

Siting IDS components

Many factors specific to the particular application can and will influence the installation and positioning of the IDS components. The following general guidance is provided as accepted good practice.

It is recommended that the manufacturer's installation instructions are followed, provided the instructions do not compromise security or conflict with CPNI advice.

Control and indicating equipment & power supplies

The control and indicating equipment (C&IE) and power supplies must be located in an area supervised by the IDS, with sufficient detection devices installed such that when the IDS is armed, access to the C&IE and power supply equipment results in a full alarm condition, (or where applicable a 'confirmed alarm'). Care is required to ensure this requirement is met when installing the control panel remote from the other system components.

IDS using a time delayed entry / exit route as part of the facility for disarming must not have the control panel located within the entry / exit route. The control panel and power supplies should be positioned in a location that is normally out of sight but accessible to facilitate maintenance. In any event, the installation of the control panel within areas to which the public have access should be avoided.

Where an IDS is divided into sub-systems of different protection levels the control panel should be located within the area supervised by the sub-system with the highest protection level.

The setting of any sub-system should also set the sub-system supervising the area in which the control panel is located.

When deciding upon a suitable mounting location for the control panel and power supplies adequate ventilation must be provided and care taken when installed not to store anything on or close to it.

Ancillary control equipment (ACE)

ACE such as keypads, token readers and displays should be positioned to facilitate easy operation by the users of the IDS. Wherever possible stand-alone keypads, token readers etc., (i.e. those intended to be located remote from the control panel), should be used.

Placing the ACE close to the final exit/entry point of the supervised area is preferred to limit the route from the point of entry to the ACE.

Care should be taken to prevent observation of the operation of the ACE by unauthorised persons (oversight). In some applications it may be appropriate to fit spy shields.

If the ACE is outside, consideration must be given to the local environmental conditions and equipment with the appropriate EN environmental classification specified, e.g. Class III or IV. If the conditions are particularly extreme, additional weather proofing can be provided.

The mounting position of ACE other than user interfaces, such as keypads, token readers and displays, should wherever possible, discourage attempts to remove or otherwise tamper with the equipment. CPNI recommends that IDS are designed and installed to be self-protecting.

Detectors

In general detectors should be installed in accordance the manufacturer’s recommendations and adjusted to provide the detection range and coverage as determined from the OR. The mounting position should where possible, discourage attempts to remove or otherwise tamper with the detector.

Moving objects that remain within the range of a motion detector when the IDS is set should be avoided as they are likely to become a source of false alarm. Care should be taken to ensure the range and coverage of a detector does not extend beyond the boundary of the area requiring protection.

Refer to the guidance on specific detector and detection technology types given in Annex A.

Alarm transmission equipment

The supervised premises transceiver (SPT) part of the alarm transmission equipment (ATE) should be located within the CIE, or in an enclosure that shares the same mains power supply, and has the same level of battery backup and tamper protection, as is required for the associated CIE, and as determined by the CPNI grading.

Alarm transmission path (ATP) aerials, network access termination points and site network equipment (SNE) that can be switched off or which has a locally or remotely accessible and changeable function, (e.g. a telephone switchboard or IP router), must be located in an area supervised by the IDS. Sufficient detection devices should be installed such that when the IDS is armed, access to the protected equipment results in a full alarm condition (or where applicable a 'confirmed alarm').

Warning devices

If used, warning devices should be located in prominent positions which are not readily accessible but allow reasonable access for servicing and effective notification of alarm conditions. The method of fixing the warning devices to the mounting surface should minimise the possibility of removal without generating a tamper alarm condition.

Interconnections to warning devices which are accessible from outside the supervised area / premises should where possible, be concealed and suitably protected against tampering, for example by enclosing the cabling within metal conduit.

Warning devices positioned outdoors should be designed and intended for external use, incorporating the appropriate weather proofing.

To avoid leading intruders to the location of the control panel, warning devices must not be placed within the locality of the IDS control panel or the SPT. Sounders built into the control panel should be disabled.

Wiring and interconnections

The use of wiring and the associated interconnections shall be appropriate for the system performance required and the local conditions within the service environment.

The installation should conform to good working practices and be in accordance with the requirements of the relevant electrical installation regulations (e.g. BS 7671[17]) as well as the specific recommendations of the equipment manufacturer(s).

All cables must be adequately supported and run in positions where there is least risk of physical damage. Cables installed below 2m above floor level and cables that may be exposed to accidental damage must be mechanically protected by ducting, trunking or conduit. Cables that drop to protective switches mounted on the floor (e.g. for the protection of roller shutter doors) should be encased in conduit to provide mechanical protection. Where the mechanical protection is made of conductive material it must also be properly earthed.

Wherever possible wired interconnections should be run inside the supervised area, however where this is impractical, interconnections shall be provided with protection against tampering, for example, by enclosing the cables in metal conduit.

It is recognised that not all enclosures for detection devices and ancillary equipment have provision to accept conduit. Where this is the case, screened cable may be installed between the conduit terminating box and the detection devices. The exposed screen shall be kept as short as possible at the point of entry into enclosures and shall be terminated at one end to a cross bonded main earth point.

The choice of cable used to interconnect the other IDS components may depend upon the specific requirements of the installation, e.g. some installation might require fire resistant cabling. However, where no specific requirements are defined, the use of a screened twisted pair type cable is preferred as it provides superior immunity to electrical interference compared with standard unscreened alarm cable.

In some circumstances mains borne electrical interference may cause false alarms. This can generally be overcome with the use of screened cabling and by filtering the mains input to the power supplies and separating interconnecting IDS cables from mains and/or high voltage cables.

Although the electrical standards require IDS low voltage cables to be run in separate containment from the mains power or high voltage cabling, it is worth confirming that adequate separation has actually been provided.

All joints in the interconnection wiring should be both mechanically and electrically secure. Where conduit access points and/or junction boxes are fitted outside the supervised area they shall incorporate tamper detection. The removal of their access covers shall require the use of a tool and the covers shall be continuously monitored by the IDS to detect unauthorised opening.

Wiring associated with alarm transmission paths (ATPs) shall be concealed as far as is practical and means provided to prevent the inadvertent disconnection of plug-in transmission connections (e.g. telephone socket with a locking facility). When ordering a dedicated connection for the SPT from the telecommunications provider, it is recommended that in addition to the telephone socket outlet, a 'block terminal' is fitted adjacent to the enclosure containing the SPT for diagnostic purposes.

Where the routing of ATP wiring may be exposed to potential lightning strikes, consideration should be given to the use of additional lightning protection devices. Many SPT devices have electrical transient suppression fitted which often requires the SPT to have an electrical earth connection. Confirmation should be sought from the alarm company that the earth connection has been made correctly to a known good earth potential. Failure to do so will result in the non-operation of the transient protection device and a very high probability of a catastrophic failure of the SPT.

The location of the antenna of a radio based alarm transmission system at Protection Level BASE or in the case of the backup transmission path of a SPT using radio frequency communications, shall where possible, be located within the supervised area and protected by the IDS. Only cable type interconnections should be used between the SPT and the antenna assembly (i.e. not a short range wireless link). All cable termination points, including those at any intermediate connections, should use termination components (or housings) that protect against cable removal without the use of a tool.

Where the antenna cannot be located within the supervised area and still achieve the recommended minimum signal strength for adequate performance, it may be installed elsewhere (preferably indoors but otherwise outdoors), subject to positioning it where its discovery and/or ready access by intruders is considered unlikely.

Any landline-based alarm transmission path (Ethernet, PSTN etc.) shall have a cable interconnection between the SPT and the first suitable alarm transmission network termination point within the premises. This interconnection shall be made in one continuous run and use termination components (or housings) that protect against cable removal without the use of a tool. The connection to the alarm transmission network shall be made in such a manner that where non-alarm related apparatus/services are also connected to that network, they do not prevent, or interfere with, the correct operation of the alarm transmission system.

For further information on interconnections, see CPNI's *Electronic Security Systems Implementation Guide*[18].

Environmental considerations

Choosing equipment that is suitable for use in the service environment is as important as selecting the appropriate CPNI grading for the IDS application.

Equipment unable to withstand the conditions of the service environment is likely to result in unacceptably high levels of false alarm or premature failure.

The requirement to protect an asset often determines where the component parts of the IDS such as detectors, need to be placed. This may be an unheated warehouse subject to wide temperature variations or other location exposed to extreme climatic change.

The European standards for intrusion detection systems include a practical series of requirements and tests to demonstrate that the IDS equipment has the ability to withstand the failure mechanisms most likely to be produced by the environment in which that type of equipment can be expected to be installed.

Compliance with these standards and tests provides a level of confidence that the equipment has the ability to operate correctly in its service environment and that it will continue to do so for a reasonable time.

The following is an extract from BS EN 50131-1[10] in which the 4 environmental classes are defined:

- **Environmental Class I – Indoor**

Environmental influences normally experienced indoors when the temperature is well maintained (e.g. in a residential or commercial property). *NOTE: Temperatures may be expected to vary between +5 °C and +40 °C.*

- **Environmental Class II – Indoor – General**

Environmental influences normally experienced indoors when the temperature is not well maintained (e.g. in corridors, halls or staircases and where condensation can occur on windows and in unheated storage areas or warehouses where heating is intermittent). *NOTE: Temperatures may be expected to vary between -10 °C and +40 °C.*

- **Environmental Class III – Outdoor – Sheltered or indoor extreme conditions**

Environmental influences normally experienced out of doors when I&HAS components are not fully exposed to the weather or indoors where environmental conditions are extreme. *NOTE: Temperatures may be expected to vary between -25 °C and +50 °C.*

- **Environmental Class IV – Outdoor – General**

Environmental influences normally experienced out of doors when I&HAS components are fully exposed to the weather. *NOTE: Temperatures may be expected to vary between -25 °C and +60 °C.*

Environmental Classes I, II, III and IV are progressively more severe, and therefore equipment meeting the requirements of Environmental Class IV may also be used in Environment Class III applications.

It is recommended that reference to the environmental classes of the European standards is made when specifying IDS equipment. However additional precautions may be necessary in certain installations, where some aspects of the environment can be identified as being unusually severe. Batteries in external warning devices may not function well (or at all) in extremely low or high temperatures.

European standards require that IDS components are labelled with the environmental classification for which they are suitable.

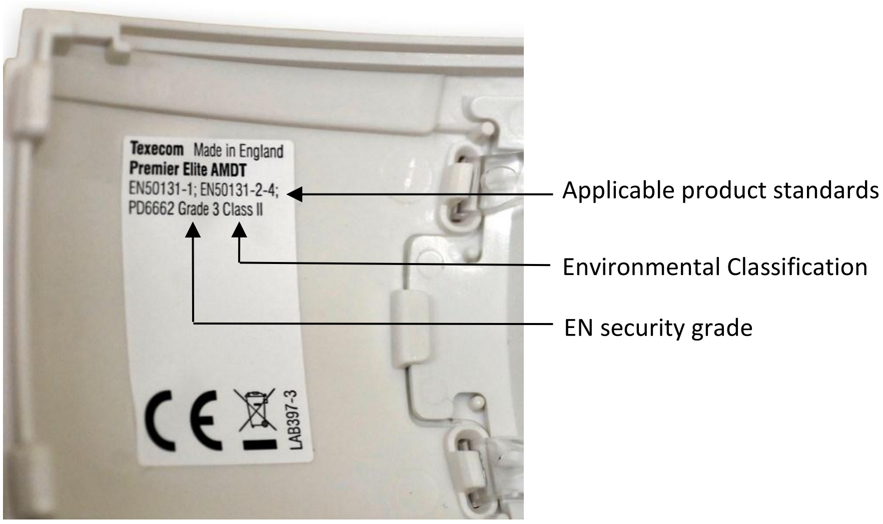


Figure 15: A product label identifying the EN security grade and environmental class. Note: the label shown is affixed to the inside of the front cover of a combined PIR and microwave motion detector.

Definitions (within the context of this guidance)

Alarm Company
An organisation providing services for IDS, including installation and maintenance.

Alarm receiving centre
Continuously manned centre to which information on the status of one or more IDS is reported. Also known as Alarm Monitoring Centre (AMC); Remote Manned Centre (RMC) and Central Station (CS).

Alarm signal
A signal which, on being received at an ARC, identifies a remotely-notified alarm condition.

Alarm transmission equipment
Equipment which is used primarily for the transmission of alarm messages from the supervised premises, transceiver interface to the alarm system interface, to the alarm receiving centre transceiver interface, to the annunciation equipment.

Alarm transmission system
Equipment and network used to transfer information concerned with the state of one or more alarm systems to one or more alarm receiving centres.

Ancillary control equipment
Equipment used for supplementary control purposes.

As-fitted document
Document in which details of the IDS actually installed are recorded.

Audibly confirmed
Designation at an ARC by interpreting audio information received from the supervised premises and determination of a high probability that a genuine alarm has occurred.

Audio listening device
Microphone mounted inside the supervised premises and used by the alarm receiving centre to provide the means to verify an intrusion is in progress.

Audio monitoring device
Component which is activated by sounds above a specific threshold.

Background checking
Monitoring of the secondary transmission path of an ATS to confirm the integrity of the communication channel between the supervised premises transceiver and the receiving centre transceiver (RCT).

Back tamper
A device used to detect the removal of an IDS component from its mounting, e.g. the removal of a control panel from the wall to which it is affixed.

Confirmation time
Time allowed for a sequentially confirmed alarm to occur after an unconfirmed alarm has occurred.

Confirmed alarm
Condition that follows after two independent actions or signals have been generated from an audible, visual, or sequential source confirming that there is or has been, a high probability that a genuine alarm has occurred.

Control and indicating equipment
Equipment for receiving, processing, controlling, indicating and initiating the onward transmission of information.

Data BUS
A cable that connects all devices on a local area network.

Digital key:
Device used for setting and/or un-setting an IDS which can be removed from the supervised premises. In the context of this guide the terms digital key and token are interchangeable.

Doppler shift
Effect created when sound wave or an electromagnetic wave is reflected off a moving object. The wave is received at frequency higher than the emitted frequency during the approach of the object and it is lower during the objects recession.

Dual technology movement detector
Detection device that employs two different sensing technologies monitored by a common processor with a common alarm output.

Duress
Notification of an alarm condition resulting from a discreet user action during un-setting without use of a HD (e.g. a special code), specifically intended for use when the user is under coercion.

False alarm
An unwanted alarm condition resulting from equipment malfunction or a disturbance within the protected area not caused by an intruder or an intrusion attempt.

Field of view
The term given to the detection coverage of a motion detector.

Final Discharge Voltage
The point at which the standby battery is discharged. If the voltage at the battery terminals falls below the final discharge voltage, the battery is over-discharged and its composition permanently changed, affecting the ability of the battery to retain further charge.

Designated entry door
Door through which entry into the supervised premises is gained.

Interconnection
The means by which messages and/or signals are communicated between component parts of the IDS.

Listen-in
Action, by an ARC, of listening to stored audio and/or to live audio received from the supervised premises.

Masked
A condition whereby the field of view of a motion detector is blocked.

Motion detector
A device able to detect and signal the presence of an intruder moving within a protected area.

Notification
Passing of an alarm, tamper or fault condition to warning devices and/or alarm transmission systems.

National Inspectorate (NSI)
A certification body for the providers of electronic security, fire safety and guarding security services.

Polling
The process of exchanging test signals by which the availability of the entire transmission path between the supervised premises transceiver and an ARC is confirmed.

Pyroelectric sensor
A sensor responding to electromagnetic radiation (infrared) whose operation is based on the pyroelectric effect, that is, the property of becoming electrically charged when heated.

Receiving centre transceiver
The alarm transmission equipment located at the alarm receiving centre or other remote centre.

Restore
Procedure of cancelling an alarm/tamper/fault/other condition and returning the IDS to a previous condition.

Sequentially confirmed
Condition emanating from two or more independent detectors, which are configured such that there is a high probability that a genuine intrusion or a genuine attempted intrusion has occurred.

Shunt lock
A switching device typically mounted within the casing of a door lock, and that is used to either, isolate an alarmed area once the door has been unlocked or initiate the IDS un-setting procedure.

Site Network Equipment (SNE)
Equipment installed within the supervised premises through which signals from the SPT to the alarm transmission network beyond the perimeter of the premises are transmitted. For example, non-alarm dedicated (shared use) IP routers, telephone switchboards/ Private Automatic Branch Exchanges (PABX), network access termination points, ATP aerials and communication network junction boxes/switches.

Specifier
An individual/corporate body responsible for stipulating the requirements IDS will be required to meet.

SSAIB
Certification body for providers of electronic security/fire systems/guarding security services.

Supervised premises
An area, a building, part of a building or multiple buildings in which an intrusion, attempted intrusion, or the triggering of a hold device can be detected by an IDS.

Supervised premises transceiver
Equipment at the supervised premises, including the interface to the IDS and the interface to the alarm transmission network.

System design proposal
Specification document for a proposed IDS, listing the equipment and components to be supplied detailing their proposed locations and containing a general indication of their coverage or purpose.

Tamper detection
Detection of deliberate interference with an IDS or part thereof.

Transmission network
A communications system between two or more items of alarm transmission equipment.

Token reader
Fixed equipment which enables the IDS to be unset using a token/digital key and which is incorporated within CIE, or ACE, or be a separate item or subsystem to provide the required functionality.

Unconfirmed alarm
Signal that has not been designated as audibly confirmed, visually confirmed or sequentially confirmed.

User - Person authorised to operate an IDS.

User interface
The means by which a user operates the IDS.

Visually confirmed
Designation by an ARC by interpreting visual information received from the supervised premises and determining that there is a high probability that a genuine alarm has occurred.

Walk test
An operational test used to confirm the detection performance of a motion detector.

Wirefree
Without wired interconnection and operating using electromagnetic fields, typically radio.

References

Standards and references

In this guide specific reference is made to the documents listed below:-

1 CPNI *Guide to Producing Operational Requirements for Measures*, February 2010. www.cpni.gov.uk.

2 *Policy Framework* (SPF). www.cabinetoffice.gov.uk/resource-library/security-policy-framework.

3 *Physical Security over Information Technology Guidance* (www.cpni.gov.uk)

4 *Catalogue of Security Equipment* (CSE).
Available from the CPNI extranet: www.cpni.gov.uk

5 **BS 4737-3.0:1988:** Intruder alarm systems. Specifications for components. General requirements (withdrawn)

6 **BS 7042:1988:** Specification for high security intruder alarm systems in buildings (withdrawn)

7 **BS 6799:1986:** Code of practice for wire-free intruder alarm systems (withdrawn)

8 **PD 6662:2010**: Scheme for the application of European Standards for intruder and hold-up alarm systems. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

9 **DDCLC/TS 50131-7**: Alarm systems - Intrusion and hold-up systems Part 7: Application guidelines. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

10 **BS EN 50131-1: 2006 + A1: 2009**: Alarm systems – Intrusion systems – Part 1: System requirements. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

11 **Low Voltage Directive** - Directive 2006/95/EC of the European Parliament and of the Council of 12 December 2006 on the harmonisation of the laws of Member States relating to electrical equipment designed for use within certain voltage limits.

12 **EMC Directive** 2004/108/EC of the European Parliament and of the Council of 15 December 2004 on the approximation of the laws of the Member States relating to electromagnetic compatibility and repealing Directive 89/336/EEC.

13 **BS 8243: 2010**: Installation and configuration of intruder and hold-up alarm systems designed to generate confirmed alarm conditions – code of practice. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

14 **DD 263:2010**: Intruder and hold-up alarm systems. Commissioning, maintenance and remote support – code of practice. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

15 **BS 8473:2006+A1:2008** Incorporating Corrigendum No. 1: Intruder and hold-up alarm systems – Management of false alarms – Code of practice. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

16 **prEN 50131-9:** Alarm systems - Intrusion and hold-up systems Part 9: Alarm verification - Methods and principles. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

17 **BS 7671: 2008**: Requirements for electrical installations. IEE Wiring Regulations 17th edition. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

18 *CNI Electronic Security Systems Implementation Guide*, CPNI 2012. www.cpni.gov.uk.

19 **ACPO Security Systems Policy 2011** - Police response to security systems. Association of Chief Police Officers of England, Wales & Northern Ireland.

20 **BS EN 50136-1-1** Alarm systems - Alarm transmission systems and equipment. Part 1-1: General requirements for alarm transmission systems. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

21 **BS EN 50131-6:2008**: Alarm systems. Intrusion and hold-up systems. Power supplies. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

22 **BS EN 50131-3: 2009**: Alarm systems – Intrusion systems – Part 3: Control and indicating equipment. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

23 **DDCLC/TS 50398:2009**: Alarm systems - Combined and integrated alarm systems - General requirements. BSI Group Headquarters, 389 Chiswick High Road London W4 4AL UK. www.bsigroup.com/standards.

24 CPNI Guidance Document - *Integrated electronic security measures*. March 2012. www.CPNI.gov.uk.

25 **The Equality Act 2010**: Available from legislation.gov.uk. Replaces the Disability Discrimination Act. Ref. www.legislation.gov.uk/ukpga/2010/15/contents.

26 **Environmental Protection Act** 1990-s79-80 Statutory Noise Nuisance and the Clean Neighbourhoods and Environment Act 2005. www.legislation.gov.uk.

Further reading

In addition to the documentation specifically referenced by this guide the security manager may find the following further reading informative.

21st Century security and CPTED - Designing for Critical Infrastructure Protection and Crime Prevention by Randall I. Atlas ISBN 978-1-4200-6807-8

Standard for Intrusion Detection Systems - Passive Infrared Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Microwave Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Active Infrared Beam Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Combined Passive Infrared and Microwave Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Glass Break Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Vibration Detectors
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Protective Switches
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Control and Indicating Equipment
Requirements for listing in the CSE. CPNI.

Standard for Intrusion Detection Systems - Shock Detectors
Requirements for listing in the CSE. CPNI

BS EN 50131-1+A1:2009	Alarm systems. Intrusion and hold-up systems. System requirements.
BS EN 50131-2-2:2008	Alarm systems. Intrusion and hold-up systems, Intrusion detectors. Passive infrared detectors
BS EN 50131-2-3:2008	Alarm systems. Intrusion systems – Requirement for microwave detectors
BS EN 50131-2-4:2008	Alarm systems. Intrusion and hold-up systems. Requirements for combined passive infrared and microwave detectors
BS EN 50131-2-5:2008	Alarm systems. Intrusion and hold-up systems. Requirements for combined passive infrared and ultrasonic detectors
BS EN 50131-2-6:2008	Alarm systems. Intrusion systems – Requirements for opening contacts (magnetic)
CLC/TS 50131-2-7-1:2009	Alarm systems. Intrusion and hold-up systems – Part 2-7-1: Intrusion detectors/Glass break detectors (acoustic)
CLC/TS 50131-2-7-2:2009	Alarm systems. Intrusion and hold-up systems – Part 2-7-2: Intrusion detectors/Glass break detectors (passive)
CLC/TS 50131-2-7-3:2009	Alarm systems. Intrusion and hold-up systems – Part 2-7-3: Intrusion detectors/Glass break detectors (active)
BS EN 50131-4:2009	Alarm systems. Intrusion and hold-up systems. Warning devices
BS EN 50131-5-3:2005+1:2008	Alarm systems. Intrusion systems - Part 5-3: Requirements for interconnections equipment using radio frequency techniques
BS EN 50131-8	Fog devices
EN 50130-4: 2011	Electromagnetic compatibility – Product family standard. Immunity requirements for components of fire, intruder and social alarm systems
EN 50130-5: 2011	Alarm systems. Environmental test methods
EN 60950-1: 2006	Information technology equipment/Safety/General requirements

Annex A: Detection technologies

Motion detection

A cost effective means of detecting the presence of an intruder is to use motion detectors. The motion detectors referred to in this section are able to sense movement within a predetermined area. The size and shape of the area, usually described in marketing literature as the ‘coverage area’ or ‘detection pattern’, is dependent upon physical properties within the detector design. By selecting a device with a detection pattern of the appropriate dimensions, a relatively large area can be protected by a single detector. This has clear advantages over other types of detection device such as protective switches and shock sensors, which will require the installation of multiple devices to cover a similar sized area. Motion detectors can provide a clear cost saving on the both equipment and installation labour.

There are various types of motion detector and this guidance manual considers those in common use. Knowledge of the basic operating principles can be invaluable when attempting to resolve problems with detectors on site, especially problems that develop long after installation and commissioning have been completed.

The following sections are intended to provide the security manager with the information to develop a basic knowledge of the operation of motion detectors, beginning with the most popular type; the passive infrared detector, commonly known as a PIR.

Passive infrared

Operating principles

Passive infrared detectors detect the presence of an intruder by sensing heat (infrared) emissions from the human body. Small levels of infrared radiation are converted into electrical signals that can be amplified and processed.

Infrared energy of wavelengths between approximately 7 to 14μm (far infrared), is focused through an optical system usually an array of lenses or multifaceted mirror (or combination of both), on to one or more tiny heat sensitive elements of a pyroelectric sensor (or the lesser used, thermopile array).

The internal construction of the pyroelectric sensor is configured such that electrical signals are only produced in response to changes in infrared levels, created for example when an intruder moves into and across the protected area.

To enable the detector to sense this movement across the entire area to be protected, the lenses or mirror facets are arranged in multiples, each providing a 'window' through which the pyroelectric sensor ‘looks out’ into the protected area.

Figure 16 provides a visual representation showing the inside of a PIR detector with the Fresnel lens cut away to reveal the pyroelectric sensor. The receiving surface of the pyroelectric sensor (coated silicon), has been lifted to expose two heat sensitive elements, these covert the infrared emissions into the electrical signals.

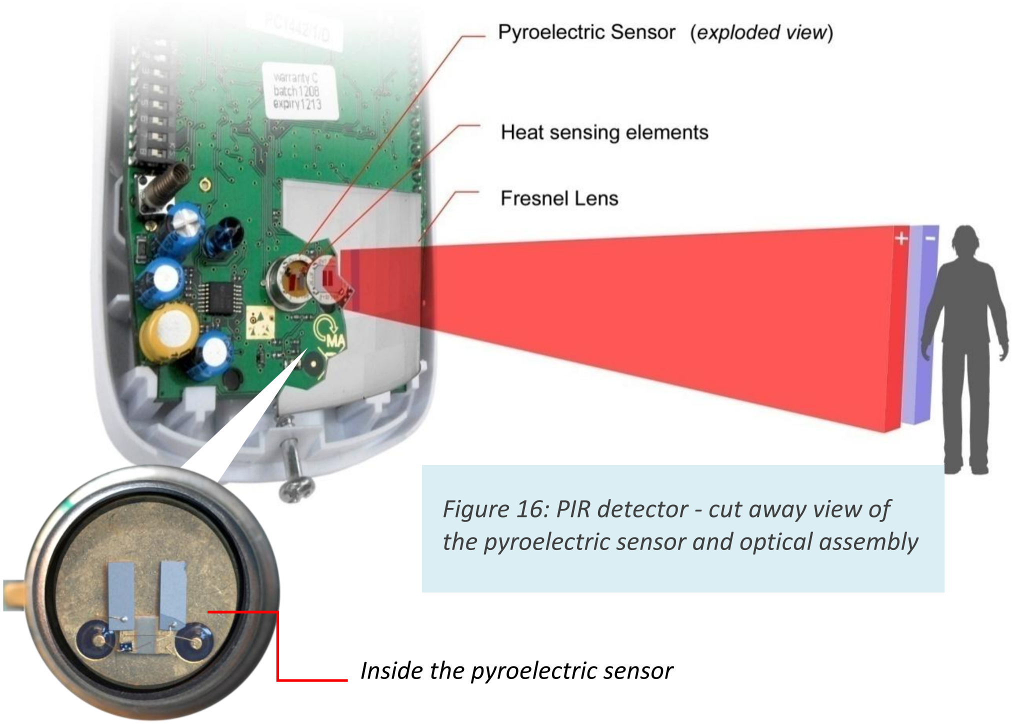

Pyroelectric Sensor (*exploded view*)
Heat sensing elements
Fresnel Lens
+
-
Inside the pyroelectric sensor

Figure 16: PIR detector - cut away view of the pyroelectric sensor and optical assembly

In the visual representation the detection 'windows' are shown as polarised 'positive' and 'negative', matching the polarity of the heat sensitive elements. It is from the changing polarity of the resultant electrical signal that the detector determines if the intruder is moving.

Sales and marketing literature sometimes refers to these ‘windows’ as detection zones, but to avoid confusion with similar terminology in the context of IDS, these are perhaps best described as sensitive sectors. The sensitive sectors are often depicted in diagrams as a series of fingers that fan out into the detection area and which converge at the detector, similar to that shown in Figure 17.

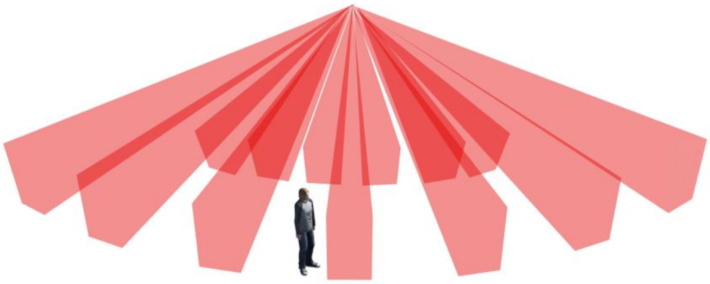


Figure 17: A diagram depicting the sensitive sectors of a wide-angle coverage PIR

The focused infrared energy appears on the heat sensitive elements of the pyroelectric sensor each time the intruder enters a sensitive sector and disappears again as the intruder exits the sector. Infrared energy from non-moving heat sources is ignored. This has the advantage of reducing unwanted alarms from stationary objects such as radiators or heaters.

Warm surfaces within the protected area such as the walls, floors furniture etc., can radiate infrared energy which is also focused on to the heat sensitive elements of the pyroelectric sensor, but since there is no movement and hence no change, these sources of heat are also ignored.

It is common for passive infrared detectors to detect differences in temperature of 2 or 3°C measured between the intruder's body and the ambient background surfaces.

It is worth adding at this point that passive infrared detectors will also respond if the intruder is cooler than the ambient background temperature, as might be experienced if the intruder enters a warm room from a cold outdoor environment whilst wearing thermally insulated clothing.

Optimum detection performance is achieved when the intruder is moving tangentially to the detector thereby intersecting the sensitive sectors.

Since the sensitive sectors fan out along radial lines from the focal point of the optics, the passive infrared detector will naturally appear more sensitive to movement across the detection pattern (field of view) rather than towards the detector. Moving towards the detector whilst walking in the gaps between sensitive sectors will permit the intruder to move quite a large distance before detection occurs, in some cases reaching to within 2m or less of the detector.

This fact need not restrict the use of the passive infrared detector, as furniture and other obstacles within the protected area rarely provide the opportunity to walk in a straight line directly towards the detector.

Application

Differing optical configurations provide a variety of detection pattern shapes, although these can generally be grouped into 3 specific categories.

1) Volumetric or ‘wide angle’ coverage

The volumetric or ‘wide angle’ is probably the most common type of detection coverage available and will probably suit most applications, typically providing a field of view just less than 90°. Other types can provide a field of view up to 180°.

Most detection pattern types incorporate multiple layers* of sensitive sectors, often staggered in arrangement to maximise the probability of detection and reduce the risk of evasion by the intruder crawling under or between the sensitive sectors.

** Note: Some single layer variants are available providing fan-shaped detection pattern with claims of immunity to the detection of pets, however these claims can be misleading. Whilst single layer detection patterns allow the movement of animals below the sensitive sectors without creating alarms, pets/animals will inevitably jump and climb onto furniture or other items which are within the detectors’ field of view. Equally, an intruder may make use of the fact that there is a large area beneath the coverage area where no detection will occur.*

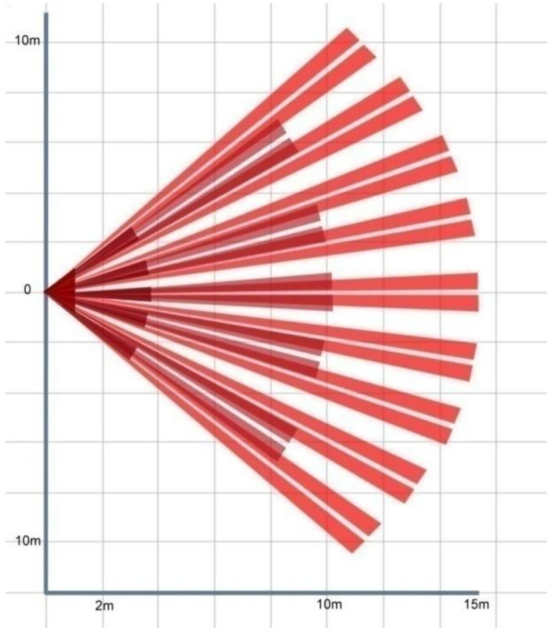
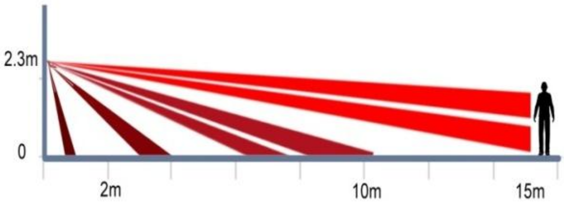


Figure 18: A wide angle (or volumetric) detection pattern. Plan view (left) and Elevated view (below)



Detection ranges can vary from approximately 2m to more than 50m (and further for PIR detectors supplied for outdoor use). For indoor use, 15m range is common because the spacing between converging sensitive sectors is optimised for good detection performance. Beyond 15m the gaps between sensitive sectors allow greater movement of the intruder before detection occurs.

Passive infrared detectors should be positioned to ensure the anticipated movements of an intruder are acrpose the detection pattern, i.e. in the most sensitive direction.

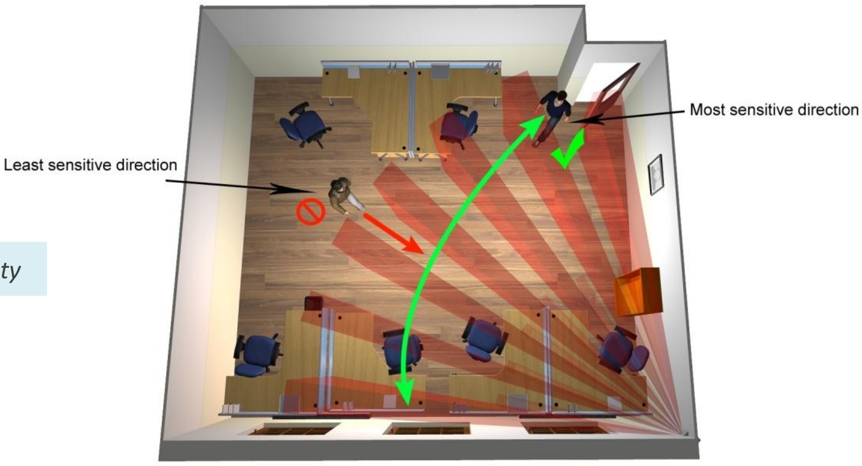


Figure 19: Directional sensitivity

Figure 19 provides an example of a detector with a wide angle detection pattern placed in the corner of a room conveniently protecting the anticipated entry points, i.e. through the windows and the door.

Since most wide angle detection patterns have a detection pattern with an angle of less than 90° (85°

is typical), assets placed close to windows may not be directly protected by the PIR. Detection will only occur if the intruder moves some distance into the room, fully crossing one or more of the sensitive sectors.

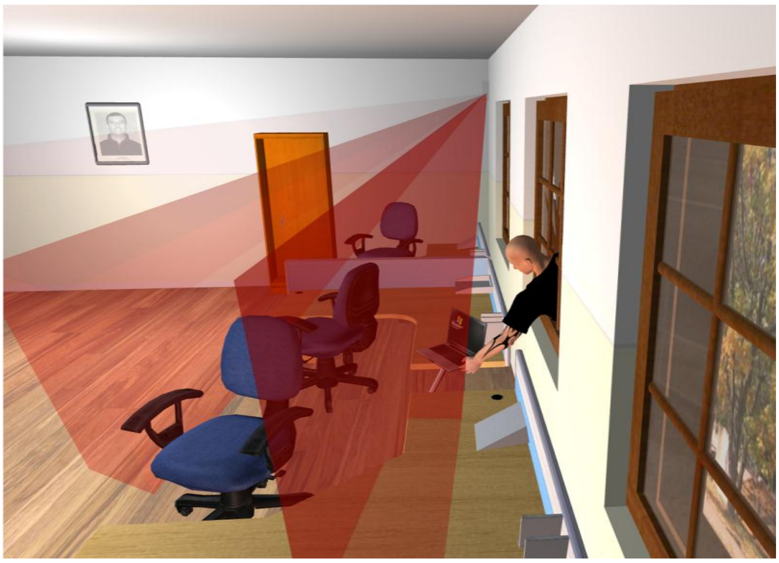
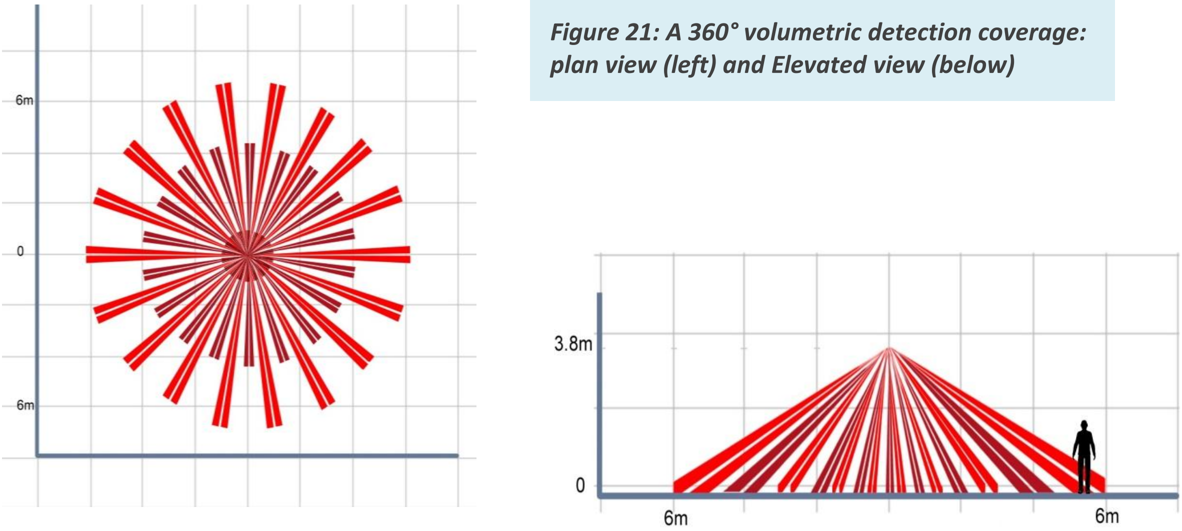


Figure 20: Assets placed close to a window may not be protected

Detectors providing 360° of volumetric detection coverage designed for ceiling mounting are also available. As relatively large areas can be protected by a single detector, 360° ceiling mounted detectors can provide cost effective solutions.

Figure 21: A 360° volumetric detection coverage: plan view (left) and Elevated view (below)



Due to the physical limitations of creating full 360°of coverage some detectors will have a relatively large spacing between the sensitive sectors which can result in the intruder being able to move a considerable distance before being detected. This may be undesirable in some applications it is therefore recommended that the product manufacturer's literature and technical specifications are studied carefully to determine the suitability of the detector prior to fitting.

2*) Long range*

Long range coverage patterns comprise a single sensitive sector, often with shorter ‘fill-in’ sectors added to detect intruders crawling underneath the main part of the coverage area. See Figure 22.

The operating distance of long range detectors intended for indoor use varies from around 20 to 60m. Longer ranges are available but may exhibit a noticeable deterioration in detection performance at, or near maximum range, particularly when moving slowly. The further away from the detector, the sensitive sectors diverge to the point where their edges no longer appear sharply defined. This results in a slow gradual change of the electrical output from the pyroelectric sensor and which is often filtered out by the electronic circuitry or the firmware, to reduce false alarms from the effects of warm turbulent air.

Long range detectors are particularly suitable for protecting continuous passage ways and corridors.

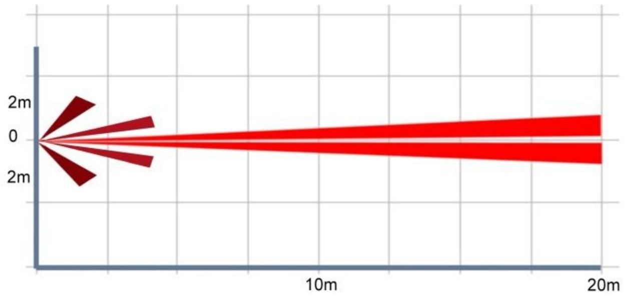
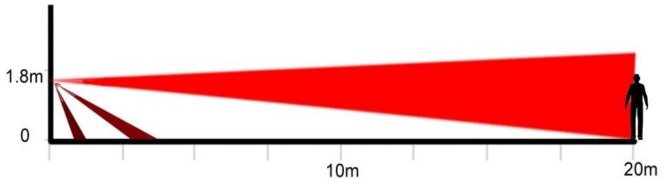


Figure 22: A long range coverage pattern. Plan view (left) and elevated view (below)



3) Curtain coverage

Detectors incorporating optics providing curtain type detection patterns generally provide a single narrow sensitive sector, similar to the shape of the long range types, but which extends continuously from the floor directly below the detector, sometimes to a point on the ceiling above (when viewed from the side), making it very difficult to pass either above or below the detector without generating an alarm condition.

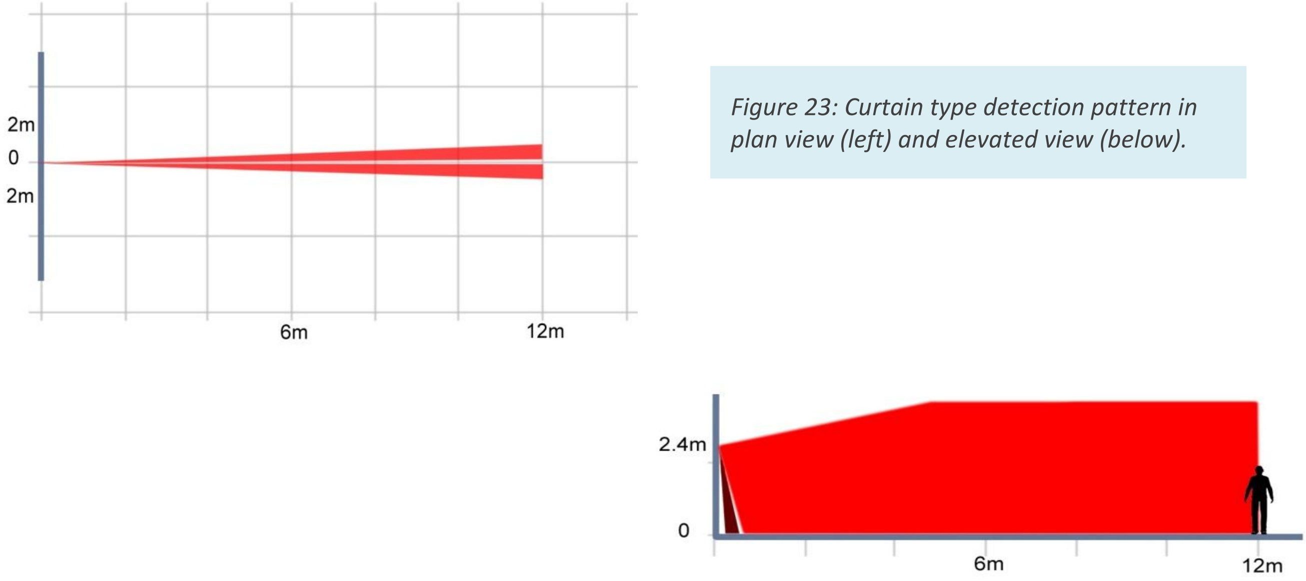


Figure 23: Curtain type detection pattern in plan view (left) and elevated view (below).

Mounting a curtain coverage detector on its side (i.e. rotated by 90°), can provide a cost-effective method of protection in roof voids or places where an intruder might be expected to drop vertically through the ceiling.

It is possible to have the continuous curtain type coverage incorporated into a volumetric detector, thus providing very a comprehensive detection pattern. See Figure 24.

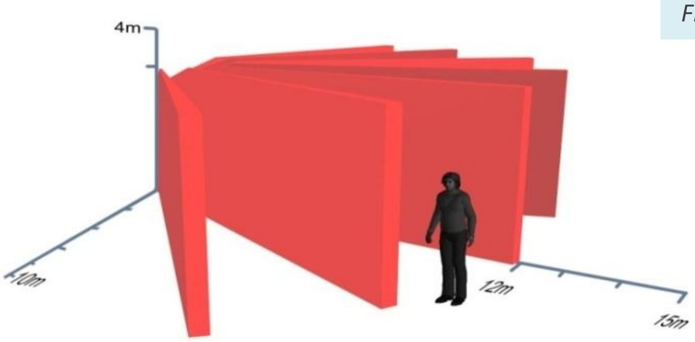


Figure 24: Volumetric curtain detection pattern

Unfortunately, far infrared is easily attenuated and so obstacles placed in the protected area might prevent the infrared emissions from reaching the detector. Care is needed when selecting the mounting location if significant blind spots in the detection coverage are to be avoided. Legitimate occupants of the supervised premises should be made aware of the consequences of placing large items of furniture or stock (e.g. boxes) within the field of view of the detector. Even detectors with anti-masking features cannot detect obstructions if placed greater than 0.5m from the detector.

Adjustments

A significant advantage of the passive infrared detector is that few adjustments are required.

Sometimes the optical assemblies can be adjusted to permit alignment of the sensitive sectors relative to the area to be protected. This is a particularly useful feature when installing long range detectors where only 1 or 2° of movement at the detector can have a dramatic effect on the detection pattern 30m away. Optical adjustment can also be used to set the detection distance by raising or lowering the lens or mirror assembly.

Early passive infrared detectors had continuously variable adjustments for sensitivity but, these have since been replaced by switches that permit the simple selection of either 'standard' or 'high' sensitivity. Their use is determined by the stability of the environment in which the detector is mounted.

A 'pulse-count' control is common. This control sets the number of sensitive sectors the intruder is required to cross before an alarm output is generated. The pulse-count feature can increase the detector's resistance to disturbances within its field of view, but care is required not to allow the intruder too much movement before an alarm output is given. Pulse-count must not be used with curtain or long range coverage patterns that have only a single sensitive sector otherwise the intruder will be able to move freely back and forth across the protected area before creating an alarm. It is noted that the insurance industry generally specify pulse-count features are disabled, as it increases detection times or even prevents detection where there is little detectable movement.

The temperature contrast between intruder and the background surfaces may be significantly reduced in the summer time when the ambient temperature is warm, making it difficult for the passive infrared detector to detect the presence of the intruder. The effects of is phenomena can be limited by using detectors incorporating ambient temperature sensing circuitry which automatically adjusts the detector's sensitivity to compensate and many of the latest models of passive infrared detector have this feature built in as standard. The product literature will generally include reference to 'temperature compensation circuitry' or similar wording.

Known causes of false alarm

False alarms are those generated by a detector in response to a malfunction or a disturbance other than an intruder entering the protected area. The nature of a disturbance that results in a false alarm may appear to the detector as a valid alarm stimulus.

Knowledge of the installation environment and careful siting of the detector can avoid many problems due to environmental disturbance. Listed below are a number of sources of environmental disturbance known to affect passive infrared detectors:

- Sunlight shining directly on to the detector can saturate the detector with high levels of infrared which can cause parts of the optical assembly to heat up and re-radiate energy at the most sensitive wavelengths, thus triggering the alarm output. To avoid this choose a mounting location where sunlight cannot shine directly on to the detector e.g. through a window or skylight.

- Sunlight shining on to a wall or floor can cause hot spots within the detector’s field of view. Although the hot spots may not actually move, clouds drifting in front of the sun casting shadows, may create the illusion of movement, and thus stimulate the detector to trigger an alarm condition. It can be particularly difficult to identify the cause this type of alarm because the sun may be in another location by the time the problem is investigated. If the cause is identified then the detection pattern should be re-aligned or the detector re-located or alternatively, changed for a different type that is unaffected by heat/sunlight.

- Heaters within the field of view of the detector can cause false alarms. Even though the heater is not moving, if it heats up unevenly the detector might interpret the output from the pyroelectric sensor as seeing a moving object. Particular attention should be paid to heaters controlled automatically by time switches. It is considered good practice to position the detector such that the sensitive sectors are aligned so that they do not 'look at' the heaters. Less obvious is the heating effect of strong sunlight on metal cladding walls which can heat up unevenly, causing the detector to activate. In any event never mount a passive infrared detector directly above a heater or heat source, because the warm air convection currents are likely trigger the detector and create a false alarm.

- Insects such as moths and spiders are known to create false alarms. Most passive infrared detectors nowadays have sealed optics preventing spiders nesting inside, close to the warm electronics. However, a moderately sized spider walking directly across the lens or on a web in front of the detector can create a large change in the received levels of ambient infrared energy. The change may be enough to generate an alarm condition. Likewise rodents (rats/mice) moving near to the detector’s lens or front window may also create an alarm event, for example if running along a shelf adjacent to and in the field of view of the detector. If this type of false alarm problem persists it may be possible, subject to the control panel installed, to logically group the outputs of two detectors. The detectors should be positioned a couple of metres apart but covering the same protected area (see also the section *Codes of practice for alarm confirmation)* The logical grouping shall be configured to require a simultaneous activation from both detectors before an alarm event is created at the CIE. Activation of a single detector within the group that does not result in an alarm notification will still be recorded in the CIE event log.

- Obvious sources of movement should be removed from the protected area when the IDS is set to ensure the risks of false alarms are further minimised. Attention should also be given to less obvious sources of movement such as that created by window blinds and curtains, which may move by the convection of air currents. Generally, re-aligning the detector's field of view away from the source of movement will resolve this type of problem. Less obvious is mounting the detector on an unstable surface which moves or not ensuring the detector mounting screws are tight. In both cases the movement of the detector can cause a false alarm.

Sometimes it is not possible re-align the field of view of the detector without incurring further problems. In such circumstances it may be possible, depending on the type of masking detection circuitry, to selectively 'mask' a single facet of a mirror or lens, effectively removing a single sensitive sector.

Adhesive tape, paint or brush-on error correction fluid, applied to the rear of a lens segment or the reflective surface of a mirror will normally be sufficient. It is recommended that in the first instance tape be used to allow adjustment of the mask until the correct positioning is confirmed, the tape can then be replaced by paint for a more permanent solution. Some detectors are supplied with masking options for this purpose.

It is recommended that details of the detectors using segment masking are recorded so that if a faulty detector needs to be replaced, the masking can be correctly reinstated to avoid a reoccurrence of the original problem.

- Most security equipment is now designed to meet the electromagnetic compatibility requirements of the EMC Directive. However, some high levels of electrical interference experienced in some service environments may still result in false alarms. Transitory electrical interference problems can be difficult to resolve. If the detector has been identified as the component being affected, the use of ferrite filters added to the supply lines and the use of screened cabling will help to improve the detector's immunity to spurious signals induced through cabling. If the problems persist consider changing the detector for a different make/model.

Protecting against attack

A limitation of the passive infrared detector is its ability to be compromised. Referring to the basic principles of operation, when the temperature difference between the ambient background (i.e. the walls and floor), and the intruder is less than the level required to generate an alarm, the presence of the intruder will not be signalled (e.g. if the intruder were to reduce his/her heat emission signature by wearing highly effective insulating clothing). Once the clothing has adopted the ambient temperature it will make the intruder appear invisible to the passive infrared detector.

This method of attack is known as cloaking. Little can be done to prevent it using only a single detector. However undetected movement across the entire protected area cannot be guaranteed because of the variation of materials which make up the background surfaces may be at different temperatures. Each material may have different emissivity properties and therefore will radiate heat differently providing an element of uncertainty. This makes cloaking a possibility, but for the intruder it is a high risk form of compromise attack, nevertheless it should not be discounted for applications requiring CPNI Class 3.

Perhaps a more likely method of attack is the application of a masking material to the front of the detector to prevent the infrared emissions from entering the detector. Materials such as paper will do this very effectively. Fortunately, some detectors have the ability to detect masking.

One method of detecting masking is to have an active near infrared emitter and receiver located within the detector's optical assembly. The near infrared is emitted either through or across the detector window (26) at a completely different wavelength from that of the heat signature from the intruder, so there is no interference with the detector's normal operation. Upon initial powering of the detector the level of active near infrared entering the receiver is measured and stored for reference. The application of masking material alters the level of infrared that is reflected back into the receiver, the change is compared with the stored reference and a masking alarm signalled.

Ideally the detector will hold the masking alarm output until its presence has been acknowledged by the user and the normal state of the IDS restored. However, some detectors restore the masking output automatically upon removal of the masking material. Detectors exhibiting this latter method of operation must be connected to control panel inputs that retain the masking event indication regardless of the status of the IDS. Also the control panel should be configured such that arming the system is prevented until the detector has been visually inspected and the masking alarm indication has been manually restored by the user.

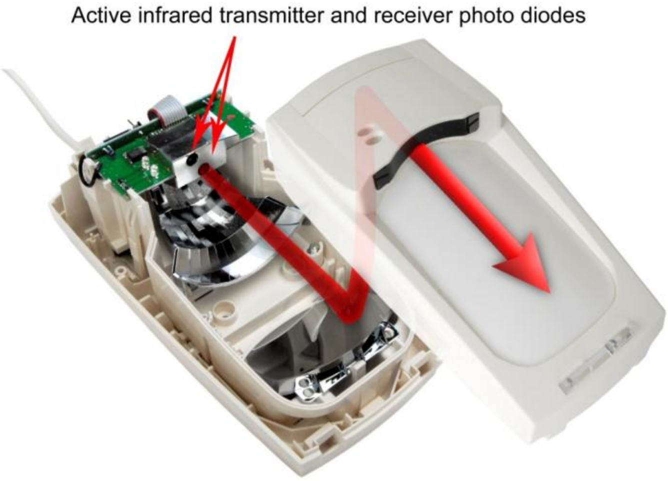


Figure 25: Masking detection

If a masking alarm has occurred, the corresponding detector must be walk tested after thoroughly inspecting it for signs of a masking attempt. Refer also the section *Detectors*.

The design of some IDS will not always permit the user to inspect detectors that have signalled a masked condition. For example, the last user to leave the supervised premises and set the IDS may not have sufficient security privileges to enter a secure area in which the offending detector is located. This situation must therefore be addressed by operating policy.

Where possible the inspection should include close examination of the detector's optical assembly. Masking may be performed using sprays and/or clear lacquer materials, the presence of which may not be immediately obvious. See Figure 10.

Most detectors are supplied with the means to detect when covers are opened and/or the detector is removed from the wall / ceiling. The detection device used is normally a micro switch with electrical contacts that open when the detector housing is opened or removed from the mounting surface.

Detecting the removal from the mounting surface (aka. back tamper) is sometimes achieved by means of a weakened section of plastic in the base of the detector which breaks out when the detector is forcibly removed. This action triggers the operation of a tamper detector device.

The correct use of the back tamper is important as it alerts users to attempts to re-orientate the detector with the intention of re-positioning the detection pattern to allow an intruder to pass undetected.

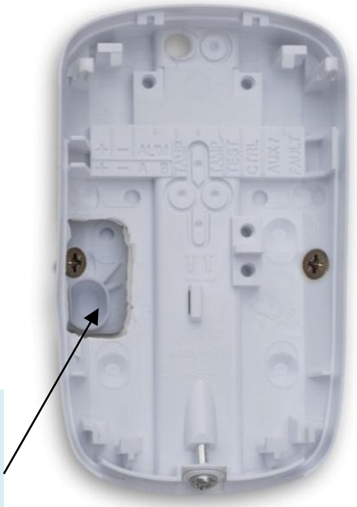


Figure 26: Back tamper. Weakened section of the mounting base that breaks out and allows the tamper detector device to operate.

Tests conducted on a range of detectors has shown that often, the weakened section of plastic associated with the back tamper does not break out as intended, preventing a tamper alarm. Where back tamper protection has been specified it is recommended that the installer cut-out the weakened section prior to installing the detector. This will ensure that removal from the mounting surface will be detected.

Detectors with steerable mounting brackets used on CPNI-graded installations should also be fitted with tamper detection devices able to signal a tamper alarm in response to unauthorised attempts to re-align the detection pattern.

Microwave motion detectors

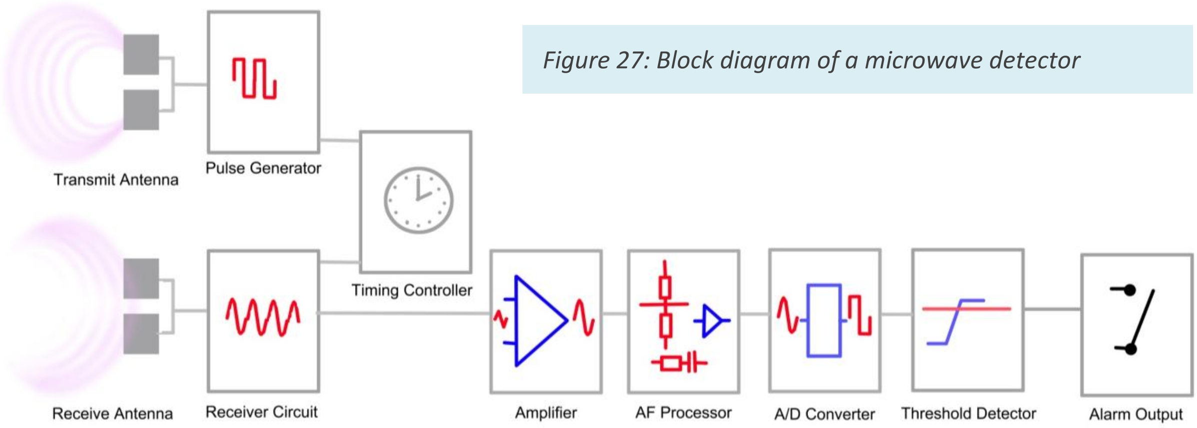
Operating principles

Microwave motion detectors emit electromagnetic 'radio' waves. When the microwaves come into contact with an object some of the waves are absorbed others are reflected and scattered in all directions and some are reflected back to the detector.

If movement is present, the frequency of the reflected waves is altered, and it is this change in frequency, known as ‘Doppler shift’ that is used to determine the presence of an intruder. The shift in frequency is proportional to the velocity of the intruder. The frequency of the microwaves reflected from stationary objects is unchanged, therefore ignored by the detector.

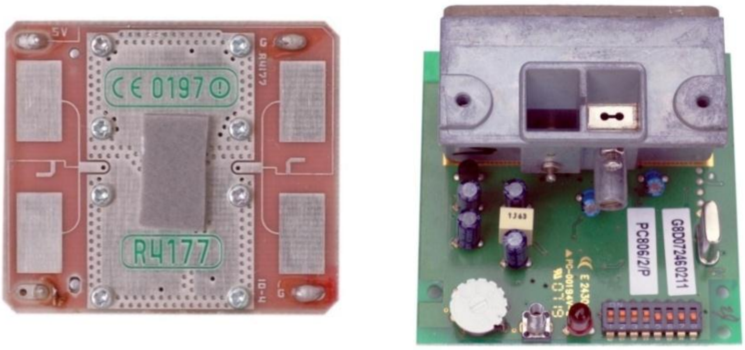
The signals from the reflected waves are very weak and so need to be amplified by the detector's microwave antenna and electronic circuitry before processing.

Figure 27: Block diagram of a microwave detector



Microwave detectors intended for use indoors usually have the transmitter and receiver assemblies combined inside a single housing and are known as monostatic microwave detectors.

Figure 28: Two types of monostatic microwave antenna



PCB antenna array

Gunn diode assembly

An example of a monostatic microwave detector

Bistatic microwave detectors are mainly used for outdoor applications and have the transmitter and receiver assemblies in separate housings.

Microwave operating frequencies are grouped into bands. The traditional band names originated as code-names during World War II and are still in use throughout the world. Common operating frequencies allocated for use with intrusion detectors are:

- 2 to 4 GHz   S-band ('S' for short wavelength)
- 8 to 12 GHz   X-band (Named X band because the frequency was a secret during WW2)
- 18 to 26 GHz   K-band (from the German word 'kurz', meaning 'short')

Detection coverage is often depicted as an elliptical pattern which is the 'theoretical' shape that can be expected if the detection performance were to be plotted in a very large room or an open space, see Figure 29. In practice the shape of the detection pattern is actually modified by its surroundings.

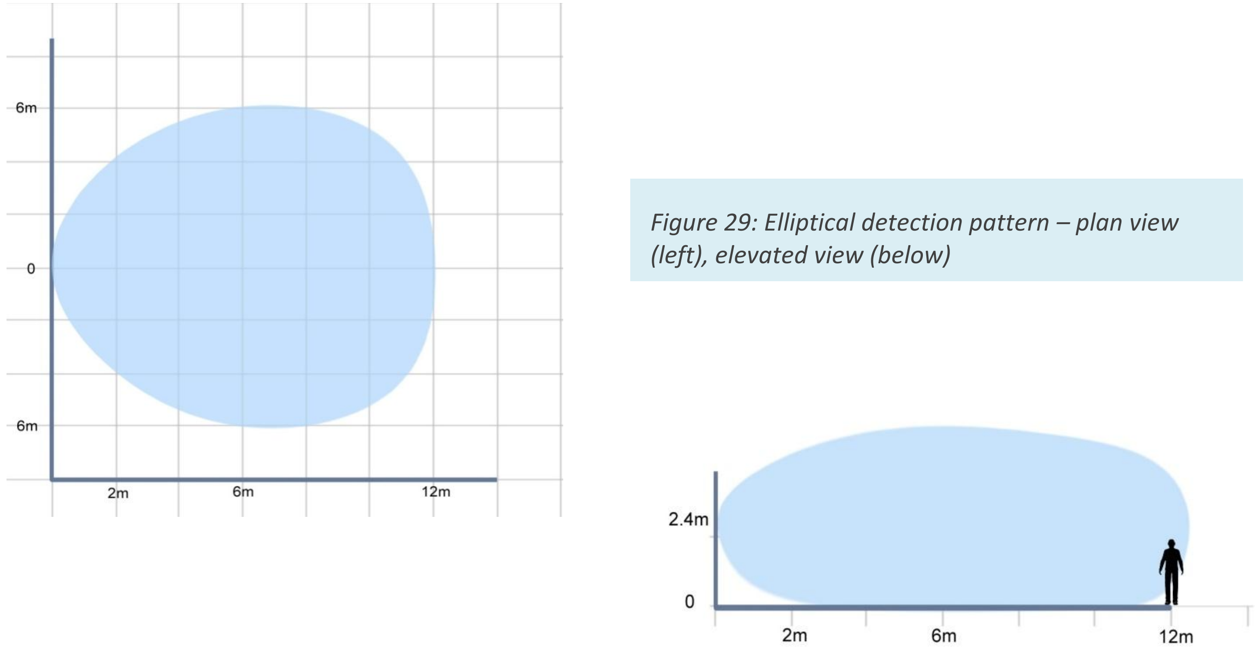


Figure 29: Elliptical detection pattern – plan view (left), elevated view (below)

A characteristic of Doppler microwave is that the detectors tend to be more sensitive to movement directly towards and/or directly away from them, unlike passive infrared detectors which respond better to objects moving across the detection pattern. Since microwaves scatter once they hit the surfaces of the walls, ceiling, floor and other objects within the room before being reflected back to the detector, the directional effect is less noticeable.

The wavelength of the microwave signals is such that microwave will either be absorbed by, or will reflect off most materials, but it also has the ability to penetrate others. This includes materials found in the construction of buildings such as plasterboard, plastics and glass, for example. Whilst this can be a useful characteristic, it can also become a source of problems.

Microwave energy penetrating the glass of a window may detect passing vehicles well beyond the protected area. Installers need to be aware of this characteristic and adjust the detectors sensitivity and range accordingly. The operation of the microwave detector may appear satisfactory during the commissioning tests, since the smaller mass of the installer or the commissioning engineer moving past the window may not reflect sufficient microwave energy back to the detector to create an alarm, whereas a bus travelling past the window on the outside of the building might.

Application

Monostatic microwave detectors are used to protect a volume, i.e. a three dimensional space within a room.

In a room free of obstacles there are unlikely to be blind spots or gaps in detection coverage. However, as most buildings contain supporting structures, furnishings and stock, etc. Adequate checks of the actual detection coverage after installation are essential.

Single technology microwave detectors are becoming harder to purchase as low production yields and rising prices of quality microwave sources have forced manufacturers to withdraw from the market. Wider manufacturing variances can be tolerated when the cheaper microwave sources are used in combined technology detectors where they will be operating in conjunction with other technology types. A single technology detector using the cheaper microwave source may experience an unacceptably high rate of false alarms.

Single technology microwave detectors offer superior detection performance compared with most combined (or dual technology) detectors, because operating in 'AND' configuration makes the detectors less sensitive (see Annex A: *Combined detectors*). It is particularly difficult to evade detection by a single technology microwave detector. Materials are available that absorb microwave energy and which significantly reduce the reflected microwaves, thus preventing detection. However, because of their size and shape the use of these materials to hide the presence of an intruder by cloaking is unlikely to provide a practical method by which to circumvent detection.

Adjustments

Careful adjustment during the initial installation and set-up is essential if the correct balance of good detection performance and acceptable immunity to unwanted alarms is to be found. Particular care is to be exercised when positioning and adjusting the detectors in locations containing materials transparent to the microwaves or that are highly reflective, such as metal sheeting.

It is common for a ‘range’ adjustment to be provided. This may take the form of a user (i.e. installation engineer) selectable parameter in a software application, a series of discrete switches or a continuously variable control (e.g. a potentiometer) housed inside the detectors enclosure. In any event access to all such adjustments should be protected by a tamper detection device.

The ‘range’ adjustment determines how far away from the detector an intruder can be detected, this is in contrast to a sensitivity adjustment which effectively sets the threshold for the number of steps the intruder is able to take before triggering an alarm. The optimum setting is one that detects minimal movement by an intruder but can still ignore unwanted disturbances occurring within the protected environment, e.g. the movement of a mouse.

The mounting location should be chosen so as to provide the quickest reaction to an intruder entering the protected area. Consideration should be given to the expected direction of movement relative to the detector orientation.

Known causes of false alarm

Care must be taken to ensure there are no objects likely to cause movement remaining within the protected area when the IDS is set.

This means checking for items such as swinging/moving signs, fans, and machines, e.g. the printing of facsimile messages. Bear in mind also that objects need not be in the direct line of sight to create an alarm. The microwave's ability to penetrate some materials could mean that the source of false alarm is not actually in the protected area at all. Water flushing through a plastic soil pipe has been known to cause false alarms.

Compared with the size of humans the effect on the reflected microwaves created by rodents is very small, however a mouse or rat moving close to the detector may cause an alarm. Small insects are less likely to create false alarms from microwave than say a PIR detector, large insects remain a possibility.

Similar to the other types of detector technologies microwave detectors can be susceptible to the effects of electrical interference. The fact that microwave detectors incorporate aerial arrays for transmitting and receiving electromagnetic energy, makes the chances of picking up stray electrical interference even more likely.

Fortunately most electrical items, microwave detectors included, are required to comply with the requirements of the electromagnetic compatibility (EMC) directive prior to being placed on the market. Compliance should provide a degree of confidence that the detector can tolerate reasonable levels of electrical interference.

The EMC performance criteria for electronic security equipment are more stringent than that applied to the average consumer type of electronic product.

Microwave detectors are not adversely affected by acoustic noise, heat, turbulent air or sunlight which makes them a good choice for applications unsuitable for passive infrared or ultrasonic motion detectors.

Protecting against attack

Microwave detectors are considered to be an ‘active’ technology in that they emit microwave energy. Changes in the levels of the microwaves reflected back to the detector can be used to detect deliberate attempts to blind the detector i.e. ‘masking’. All detectors for use in CPNI-graded applications requiring products to Protection Level ENHANCED or HIGH and all Class Ratings must incorporate masking detection.

As previously stated, materials are available that could be used to cloak the intruder in an attempt to evade detection but the use of these material is cumbersome and unlikely.

Microwave detectors can have adjustable mounting brackets, either built into the housing or supplied as an option to aid alignment. If adjustable mounting brackets are used, it is important that these are sufficiently robust to resist deliberate attempts to alter or re-orientate the direction of coverage. A tamper detection device may be fitted which signals a tamper alarm condition if the bracket is re-aligned or moved. Alternatively, the bracket could deliberately shear if forced thereby rendering the detector and bracket unusable and leaving an obvious visible sign that it has been tampered.

It is recommended that detectors with adjustable mounting brackets used in CPNI-graded installations be fitted with tamper detection devices that operate if the orientation is altered by force.

Combined detectors

Operating principles

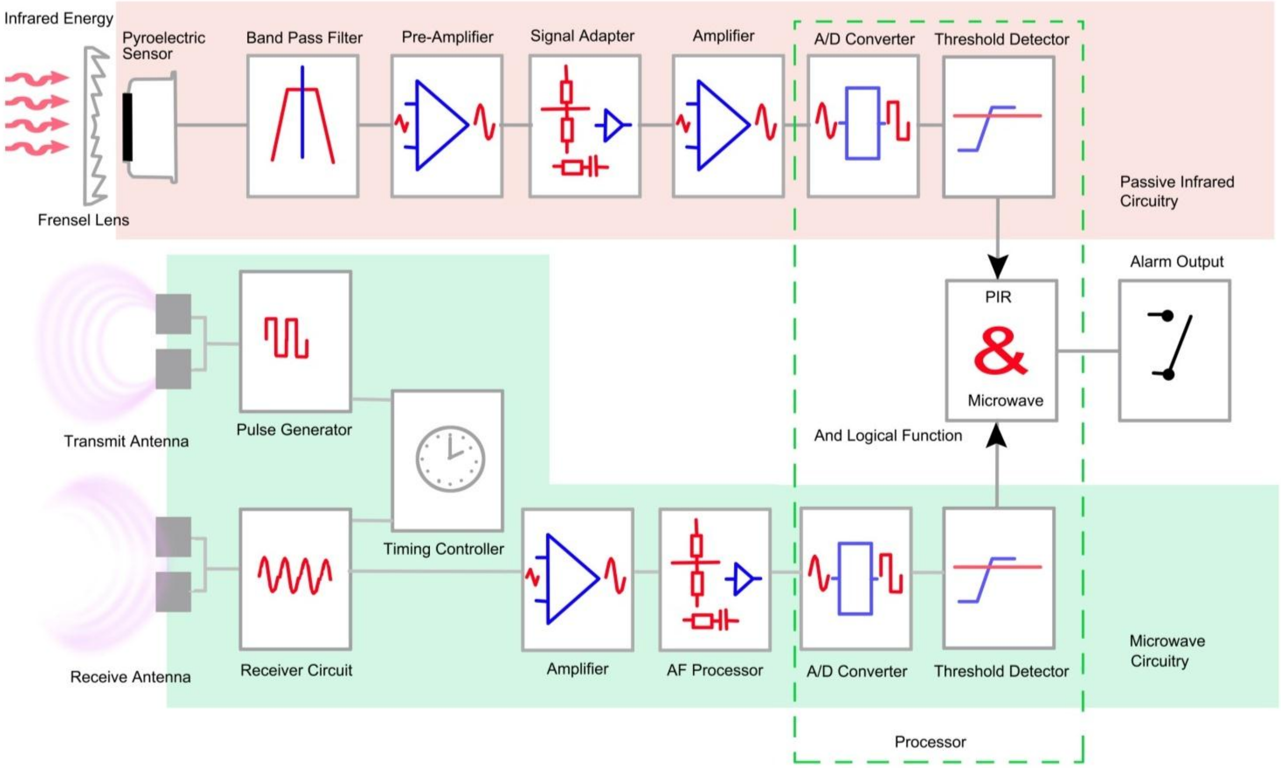
Detectors incorporating two or more detection technologies in a single housing, e.g. passive infrared combined with microwave, have become popular because of their increased stability in the service environment. Commonly referred to as dual technology or 'Dual Tec' detectors, the combination of differing technology types provides the benefit of increased resistance to false alarms compared with detectors of only a single technology. The most common combined detector is the passive infrared combined with microwave, designed to operate in ‘AND’ configuration. Only when both detection technologies shall have sensed movement within a predetermined time window will an alarm output be generated, see Figure 30 on page 73.

- **Passive infrared and microwave**

The pairing of passive infrared with microwave detection technology can provide improved immunity to false alarm, for example the unwanted effects of heat sources, turbulent air, sun light reflections etc. will not influence the microwave. Similarly, the problems associated with the transmission of microwaves beyond the desired detection area, by penetrating glass for example, are significantly reduced because the passive infrared is unable to 'see' through the glass.

Furthermore, the two differing technologies are both sensitive to movement but in different directions (i.e. perpendicular). In theory passive infrared and microwave detection working together requires an element of movement in both directions for an alarm to be signalled, e.g. movement diagonally across the detection area. This further increases the stability of the detector to unwanted disturbances in the service environment.

Figure 30: Block diagram of a combined PIR and microwave detector



In practice the intruder will still be detected even if traversing perpendicular to the detector, due to the reflected microwaves scattering in all directions within the protected area. Generally however, combined detectors operating in 'AND' logic mode are perceived to be less sensitive to intruder movement than detectors incorporating only a single technology.

Some manufacturers have implemented more complex algorithms for combining the received PIR and microwave signals, instead of a simple 'AND' logic function the detector may, for example enhance the sensitivity of the passive infrared circuitry in response to activity sensed by the microwave.

Although the pairing of passive infrared and microwave is by far the most common, other technology combinations are available;

- **Passive infrared and ultrasonic**

Ultrasonic sensors also use Doppler Shift principles but at frequencies between 25kHz and 75kHz. Sound waves above human hearing are emitted into the protected area and reflected back to the detector by bouncing off solid objects (such as the surrounding walls, floor, ceiling and room furniture). The reflected waves are picked up by an ultrasound receiver transducer also housed within the detector housing.

Objects with hard surfaces tend to reflect more of the ultrasound, while soft surfaces tend to absorb it. Therefore, better detection performance can be achieved when installed in an area where fewer soft furnishings are present.

Performance can also be influenced by climatic conditions, in particular the amount of moisture content in the air. Climates with high humidity tend to reduce the detection range of ultrasonic detectors, although this effect is not noticeable in the UK.

Few ultrasonic combined detectors exist nowadays due to the superior performance of the modern passive infrared and microwave devices. Single technology ultrasonic detectors are no longer manufactured.

- **Passive infrared and infrasonic**

Infrasonic devices sense changes in air pressure within the protected volume. Changes in air pressure can be created when a window is smashed or an external door opened forcibly.

When combined with passive infrared detection technology and using 'AND' logic, an alarm condition will result following a forcible entry and subsequent movement by an intruder in front of the passive infrared sensor.

Unfortunately infrasonic detectors have been known to trigger on changes of air pressure created by gusts of wind passing over the outlet of a flue pipe or the top of chimney. The sudden gust creates a vacuum effect which can result in pressure change inside the protected premises, this can be sufficient to trigger the infrasonic sensor.

Conversely, infrasonic detectors may not react at all if the entry by the intruder fails to create a change in air pressure. For example, by entering the protected premises without using force or by opening slide or tilt and turn style windows where the air displaced is effectively balanced as the windows are opened.

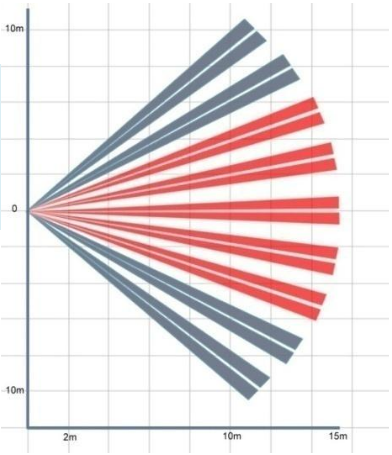
- **Dual passive infrared**

Dual passive infrared detectors are sometimes categorised as combined detectors even though they do not incorporate different detection technologies. They comprise two independent passive infrared detectors located together in a single housing.

The requirement of BS 8243 for non-overlapping detection patterns* has been the driver for this type of detector as they were thought to provide a cost effective means to comply with the sequential alarm requirements; saving on both equipment and installation costs.

** When installing a single detector that provides two independent non-overlapping detection patterns to the requirements of BS 8243, its use must be declared to the response authority.*

Figure 31: Non overlapping coverage pattern (plan view). An example of a single detector that provides two independent non-overlapping detection patterns.



No single environmental disturbance shall result in a confirmed alarm so by ensuring the detection coverage patterns of the two detectors do not overlap, the occurrence of a single disturbance, such as a sign swinging in front of one of the detectors, is less likely to trigger both detectors thereby resulting in a confirmed alarm event.

Best practice is achieved by mounting two separate detectors some distance apart (>2.5m), as it can be argued that mounting the two detectors in the same housing will not prevent a confirmed alarm being signalled by a single disturbance such as a moth fluttering close by, or a spider walking across the front of the detector.

- **Passive infrared and CCTV**

Although less common than other types of combined detector there are an increasing number of devices that pair passive infrared technology with a small camera. The camera may be used to provide evidence as to the cause of the alarm, in the form of a series of still images before and after the detector activated or video footage of the actual event. Alternatively the camera may be used to memorise the image of the protected area with the view to establish if objects have been placed in front of the detector that may block or impede its field of view.

Since the same or better performance can be achieved with relatively low-cost, IP-based cameras coupled with suitable video analytics, the longer term future of the combined passive infrared and CCTV detector is uncertain.

Application

Typically, most combined detectors have wide angle/volumetric detection patterns, although it is possible to obtain long range and 360° types from some manufacturers.

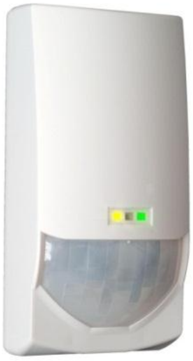
Installation guidance and best practice advice is similar to that recommended for the single technology detector types.

Adjustments

Whilst combined detectors may be inherently more tolerant of disturbances in the service environment than single technology detectors, careful adjustment and set up is still required to achieve optimum reliability and performance. Even though two or more detection technologies are being used together, the microwave should be adjusted to minimise the possible penetration through materials that are transparent to its wavelength. Commissioning tests should confirm there is no activity from the microwave detection technology caused by objects/people moving outside the protected area. Equally, general false alarm avoidance precautions should also be followed for passive infrared technologies to minimise the possibility of unwanted alarms.

Most combined detectors incorporate visible indicators which when enabled, display the activity detected by each of the detection technologies independently. This can be a really useful feature when commissioning the detector or when performing confirmation checks.

Figure 32: Illuminated LED indicators displaying activity on both the microwave and passive infrared detection channels



Mounting locations must be strategically chosen to achieve the fastest response to an intruder entering the protected area. Anticipated entry points such as doors and windows etc., must be considered.

As a rule of thumb, where passive infrared and Doppler type technologies are used together, the combined detector will respond quickest when the direction of movement of the intruder is at 45° to an imaginary radial line drawn from the detector. See Figure 33.

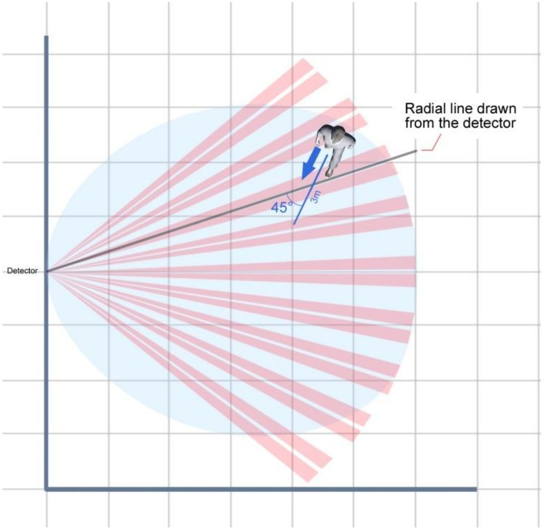


Figure 33: Radial line drawn from the detector

Known causes of false alarm

Even though combined detectors are inherently more tolerant to disturbances the same degree of care needs to be afforded as if a single technology detector were being used.

Combined detectors of differing technologies that require both technologies to have been triggered simultaneously (or within a timed window) will have increased immunity to many of the known sources of unwanted alarm discussed earlier.

Sunlight and other forms of heat source would not disturb the microwave sensor since the microwave will not react to heat or changes in infrared levels, nor ambient light, therefore no alarm output will occur even if the passive infrared technology triggers in response to any of these stimuli.

Spiders are unlikely to trigger both the microwave and passive infrared sensors simultaneously, however rodents and possibly moths could still cause unwanted alarms if they move close to the detector. However, the risk of false alarm is much reduced.

Small levels of movement within the field of view, such as window blinds or curtains swaying due to the effects of convected air currents are likely to be tolerated by a combined passive infrared and microwave technology detector. In general, the pairing of these technologies results in the need for a greater level of movement before the disturbance is sufficient to create an alarm. However, a stack of boxes toppling over in front of the detector could still be expected to trigger an alarm output.

False alarms triggered by electrical interference remains a possibility even with combined detectors.

The desire to 'value engineer' products to control costs has resulted in some combined detectors being manufactured with sensor circuitry that may otherwise have been unsuitable for use in a single technology detector alone. Instabilities within the design increase the risk of false alarm but when paired with a differing technology and configured with an ‘AND’ logic, an acceptable level of performance can be obtained. None-the-less the overall reliability will not be as good as a combined detector made with two (or more) high quality sensors.

Protecting against attack

Combined detectors incorporating passive infrared technology and operating in a logical ‘AND’ configuration will adopt the limitations of the passive infrared detector to compromise attack. If the heat emissions from the intruder are obscured, the passive infrared circuitry might not detect the presence of the intruder and therefore no alarm output would be given by the combined detector.

Detectors incorporating two active technologies such as ultrasonic and microwave Doppler, perform better against intruders trying to evade detection. Unfortunately there are very few of these types of combined detectors on the market. Most have become obsolete in favour of the popular combined passive infrared and microwave combination.

Regardless of the technologies used, all detector types should incorporate a means to signal a tamper alarm upon removal of the detector from its mounting surface and when the housing is opened. This will significantly reduce the possibilities of an undetected compromise attack, i.e. by manipulating the electronic circuitry or by masking (‘blinding’) the optics form inside the detector. Combined detectors suitable for use at Protection Level ENHANCED and HIGH and all Class Ratings will incorporate ‘masking’ detection circuitry, similar in design to that used on the single technology products.

Glass break detectors

Sometimes there is a need to incorporate into the IDS the means to monitor glazing to detect forced entry, be it through windows, doors, skylights or even display cabinets. Glass break detectors are used for this purpose.

Operating principles

When glass breaks it generates a wide range of frequencies, ranging from infrasonic, i.e. below 20 Hertz (Hz) and which cannot be heard by the human ear, through the audio spectrum 20 Hz to 20 kHz, right up to ultrasonic i.e. above 20 kHz and beyond the range of most humans' hearing. Depending on type, glass break detectors use the frequencies in one or more of these bands to detect the breakage.

⚠ The use of blast resistant film may significantly impair the operation of the glass break detector. However some makes of detector are able to function correctly with the film present. In all cases specific advice must be sought from the manufacturer.

Several types of glass break detector are available, as explained in the following sections.

Metallic window foil and alarm glass

Metallic window foil comprises a strip of very thin electrically conductive aluminium, approximately 9mm wide, which is stuck to the glass to form an electrically conductive loop and brushed with a protective polyurethane coating. A connection from the IDS control panel to the conductive foil is made via screw terminals mounted on self-adhesive blocks also stuck to the glass.

When the glass is broken the brittle conductive foil tears, thus interrupting the electrical circuit. The control panel interprets the interruption as an alarm condition. Although simple, metallic window foil does not offer resistance to compromise attacks since the foil and often the terminations remain exposed. The foil can also be damaged accidentally whist cleaning the glass. For these reasons the use of metallic window foil is not recommended.

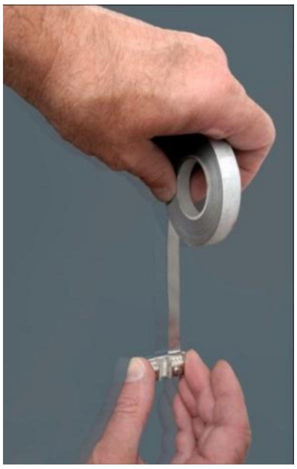


Figure 34: Metallic foil

Alarm glass offers a more robust solution. Alarm glass has a conductive circuit sandwiched between the laminated layers of sheet glass. Being inside the glass the conductive circuit is less prone to accidental damage and attack. The terminations can be hidden from view within the window/door frame making them less accessible. The principles of alarm glass is similar to that of conductive foil, an electrical circuit is interrupted when the glass is broken.

Alarm glass is the most reliable of all the glass break detector types, but the glass has to be manufactured to order and so is often considered cost prohibitive when compared with other solutions.

Acoustic glass break detectors

Acoustic glass break detectors are mounted in relatively close proximity to the glazing and continuously monitored for specific frequencies associated with the sounds of breaking glass.

Some of these devices detect the acoustic signature that is created when the glass first flexes, cracks and then shatters into many pieces and falls to the floor.

Such precise discrimination improves resistance to false operation but there is a risk that the device can be fooled relatively easily by the intruder dampening some of the frequencies made by the breaking glass. Applying self-adhesive film to the glass before breaking it for example, will absorb the higher frequencies and prevent the glass fragments from falling, thereby avoiding the resultant tinkling sound normally made as the glass hits the floor.

With typical detection ranges between 5 to 10m (i.e. the radial distance measured from the detector to the glass), the use of acoustic glass break detectors can provide a cost effective solution. A single detector can monitor a relatively large glazed area comprising many small panes of glass and without the need for wiring to each individual pane of glass.

Figure 35: Acoustic glass break detector

It is important that the manufacturer’s recommendations are followed regarding suitable glass types and where best to position the detectors. Not all acoustic glass break detectors respond to all types of glass, polyvinyl butyral layers within laminated glass for example, may affect the range of high frequency sounds produced as the glass breaks.

The acoustics within the protected area will also have a significant effect on the transmission of the sound and subsequently affect the detection performance. Soft furnishings will absorb the high frequencies resulting in the detection range being reduced.

Careful consideration must be given to the effect on the operation of the detector if changes are made within the protected area after installation, which alter the acoustics, for example the addition of windows blinds or heavy curtains.

Acoustic glass break detectors can be compromised relatively easily by preventing the sound waves reaching the detector, either dampening the sound created when the glass breaks or by covering the microphone aperture(s) in the detector housing.

Hand operated test devices are available for some types of acoustic detectors to facilitate regular checks to confirm correct operation over the detection range.

Piezo electric glass break detectors

Piezo electric glass break detectors comprise a piezo electric element affixed to a metal or ceramic substrate, which during installation is glued to the surface of the glass inside the supervised area. When the protected glass breaks the substrate and the piezo electric element physically flex causing a minute electrical charge to be generated. The charge is amplified and the resulting signal analysed to determine if an alarm is to be signalled.

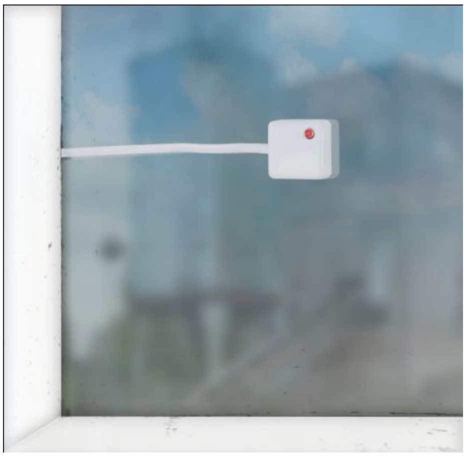


Figure 36: A piezo electric glass break detector

These detectors are generally easy to install, with no adjustment required.

Tools are available to aid the correct positioning of the detector on the glass whilst it is glued in place.

Some manufacturers also provide test tools to enable the detection performance to be checked - clearly a useful feature since actually breaking the glass to test that the detector is working would be undesirable.

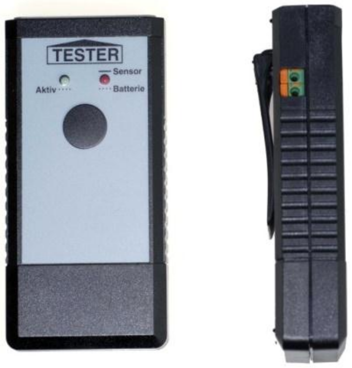


Figure 37: Glass break detector test tool

Manufacturers of piezo electric glass break detectors recommend that the detectors are discarded once the glass to which they are affixed has been broken, and a new device fitted when the glass has been replaced.

Modern adhesives can create a very strong bond between the ceramic/metal base of the detector and the glass but after years of exposure to the ultra violet rays of the sun the bond can deteriorate. For this reason detectors should be checked regularly during audits to confirm that they remain firmly attached to the glass. This type of glass break detector has only one chance to detect the initial crack of the breaking glass and if it is not in good contact with the glass it will not create an alarm.

The majority of piezoelectric type glass break detectors on the market have no means to monitor if they have become separated from the glass either accidently or by deliberate act, i.e. they have no back tamper and therefore cannot alert the IDS to a compromise attack. Sometimes integral tamper detection wiring loops are provided but these will only operate if the interconnecting cable to the detector is severed. Equally, if the detector has fallen off the glass by accident, the IDS does not know.

It is important to ensure the protected glass is maintained in a good condition, loose, cracked or broken glass might cause false alarms and so should be replaced as soon as it is noticed.

Similar to acoustic types the detection performance of piezo electric glass break detectors can be impaired if the glass contains properties that have a dampening effect on the high frequency signals created when the glass breaks, e.g. laminated safety glass.

Specific makes/models of detector may be better suited to particular types of glass than others, therefore it is important the glass type is identified and the detector manufacturer consulted and the recommendations followed.

Piezo electric type glass break detectors are relatively inexpensive (when compared with the other glass break detection technologies), and so can provide a cost efficient solution. This will of course be subject to the size and quantity of the individual glazed panels to be protected. Where the glazing consists of multiple individual panes of glass, one detector will be required for each glass pane, thereby rapidly increasing installation costs.

Active glass break detectors

Unlike the other types of glass monitoring devices, active glass break detectors emit energy in the form of ultrasonic oscillations transmitted across the glass to one or more ‘receiver’ transducers.

Fractures or breaks in the glass can reflect and/or attenuate the transmitted ultrasound signals, either way a change occurs to the signature of the ultrasound oscillations. The sensitive electronic circuitry of the detector compares the distorted signature characteristics received with the signature of original transmission. An alarm is signalled if the distortion exceeds a predetermine value.

An alarm condition is also created if the detector fails to receive the ultrasound oscillations. This can occur if either transmitting or receiving transducers become detached from the glass. Such a feature offers a clear advantage over the other types of glass break detector discussed, as tampering or the accidental removal of the detector from the glass can be signalled.

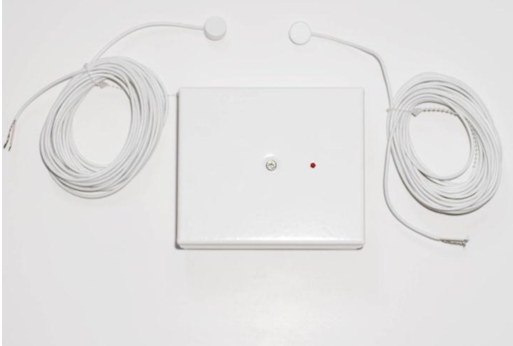


Figure 38: An active glass break detector and transducers

Calibration to the specific application enables the use of active glass break detectors with a range of glass types, laminated, tempered (toughened glass), wired, ballistic resistant and normal float glass for example. However, the specific recommendations of the detector manufacturer should be followed where possible.

Known causes of false alarm

To avoid false alarms acoustic glass break detectors should be used only where the ambient noise levels are low when the intrusion detection system is set. Sounds produced by metallic objects such as security grilles clanking together, or glass bottles rattling, and some types of bell are known sources of false alarms as are the sirens of emergency vehicles.

Break glass detectors should be located where interference from the public is prevented. Piezo electric types are sometimes used to protect shop fronts particularly jewellers, but there is a risk of false alarms generated deliberately by people tapping on the outside of the glass with metallic objects such as coins.

Vibrations caused by heavy traffic may also give rise to a false alarm as will hail stones striking the window. Although the use of double glazing significantly reduces the risk of false alarms from hail stones provided it is only the inner layer of glass that is being monitored by the detector.

Loose, cracked or broken glass is a potential source of false alarm for all types of glass break detectors.

Protecting against attack

If the threat level is such that there is a genuine risk the glass break detectors may be exposed to a compromise attack, then the use of the active type of glass break detector is recommended along with fully supervised alarm and tamper loops back to the control panel.

It is recommended that the operation of the tamper detection circuits including the interconnection wiring junction boxes are demonstrated during the handover procedure. See *System handover* section.

Vibration and shock detectors

Vibration and shock detectors are used in applications where the expected intrusion attempt will result in the penetration of a planar surface (e.g. a wall) or other type of barrier, using techniques such as drilling, impacting with a sledge hammer, pick axe or similar tool, cutting with a saw or grinder or oxyacetylene torch/rope, possibly even blasting with explosives.

Operating principles

The detectors can be categorised into the following 3 types of device:

1. Seismic devices contain one or more piezo electric elements that produce an electrical charge when flexed physically. Attached to a suitable mechanism the piezo material's ability to generate electrical signals can be used to detect the presence of vibrations.

2. Modern types of **inertia sensor** use innovative designs to sense vibration but the basic principles of operation can be explained by depicting a small metallic ball resting on a set of electrical contacts, see **Error! Reference source not found.**Figure 39. When the ball is at rest it completes an electrical circuit between the contacts. The continuous electrical circuit is interpreted by the electronic analyser circuitry as a quiescent non-alarm condition.

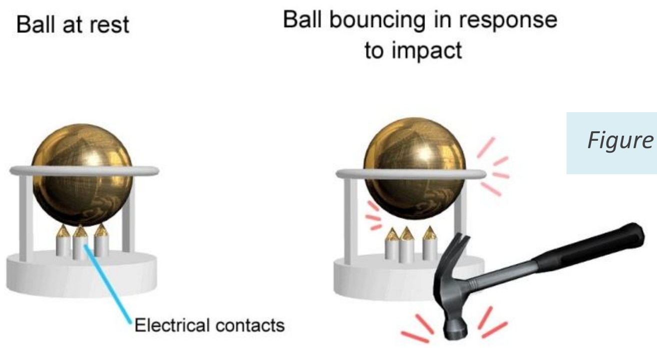


Figure 39: Inertia sensor - principles of operation

Because the ball is free to move with the inertia created by an impact to the substrate on which the detector is mounted, the ball jumps off the contacts, thereby interrupting the electrical circuit momentarily. The interruption is of a very short duration but measureable by the analyser circuitry. A succession of multiple interruptions will be interpreted as an attack signature and an alarm condition generated.

3. Shock sensor technology may use either the seismic and inertia technologies described previously or a solid state accelerometer arrangement to produce small electrical signals upon which the processing circuitry can determine if an alarm is to be generated.

Shock sensors normally respond to vibrations created from forcible entry styles of attack that create short bursts of high intensity energy, e.g. smashing a door from its hinges.

When selecting vibration or shock detectors it should be noted that there may be inconsistencies with the terminology used in the marketing/sales literature. Not all literature clearly distinguishes between the different types of detection technologies in the way they have been described above, and often mix up the terms and definitions.

Seismic detectors

Seismic types of vibration detector are able to detect a wide range of forcible attacks, from high intensity shock impulses down to minute vibration tremors. Seismic detectors are used mainly to protect safes, automatic teller machines (ATMs) and strong rooms where the range of attack methods and tools vary significantly. Some models may also be used for general purpose applications providing the mounting substrate is of solid construction, walls made with good quality engineering bricks for example. Insulation blocks tend to dampen the transmission of the vibrations and have the effect of reducing the detection range.

Seismic detectors designed for safes and strong rooms are at the higher end of the price range, so protecting a large area of perimeter walling will quickly become cost prohibitive.

With the appropriate installation design and configuration settings most devices can be made to discriminate between the vibrations created by a genuine physical attack and relatively high levels of ambient background vibration noise that might be present in the service environment.

Figure 40: A seismic detector

A typical example is a detector fitted to an automatic teller machine (ATM), it must ignore traffic noise and the vibrations created whilst the machine counts the money prior to dispensing it, yet still respond quickly in the event of an attack intent on breaking opening the ATM.

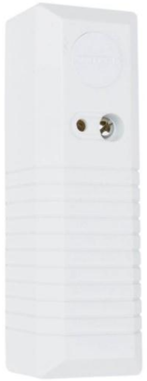
Seismic detectors are able to detect attacks using impact, drilling, cutting and thermo-chemical (i.e. Thermic lance) methods. Some incorporate specific circuitry and firmware to detect the powerful and short duration shock waves created by explosions.

Accessories are often available that provide enhanced protection to safes and ATMs. These are usually sliding or rotating covers arranged to cover keyholes or to obscure the combination tumbler spinner of code locks. The slides are arranged to activate a micro switch within the detector when moved and thus provide an additional method of detection. The slide may also have a solenoid arrangement to prevent it being moved once the alarm system has been set.

Inertia detectors

Inertia detectors are designed more for general purpose use where they can provide a reliable and cost effective solution for the detection of most methods of forcible entry.

Blast, impact, drilling and some types of cutting attack can be detected by inertia detectors.



Where supplied with sensors which are separate from the analyser circuitry, multiple sensors can usually be connected to a single analyser thus significantly extending the area of detection coverage.

Figure 41: An inertia detector

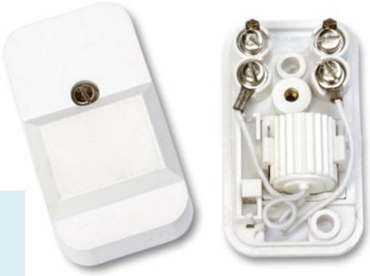


Figure 42: Remote inertia sensor

Shock detectors

Shock sensors are best used for the detection of 'gross' physical attack methods such as impacting. Some types of shock sensor will also detect explosions. Where doubt exists about the detector's capability the manufacturer should be consulted.

Application

To select the right type of vibration detector it is necessary to know as much as possible about the structure to be protected, the material from which it is made, whether it is modular or of homogeneous construction.

The optimum transmission of vibration is achieved when there are no cracks or breaks within the structure. This can be difficult to determine particularly if a wall is rendered or has some other form of external finishing. Clearly, materials that absorb vibration such as rubber surfaces are best avoided.

It is also necessary to have an idea of the likely methods of attack that might be used, as this will also determine which type of detector is most suitable.

Sealed intrinsically safe types may be required for protection of environments containing explosives.

Since detection performance is entirely dependent upon the transmission of vibrations it is essential to have good physical coupling between the detector and its mounting surface. The use of long fixing screws or an anchor bolt secured deep into the wall/substrate can help channel the vibrations to the sensor.

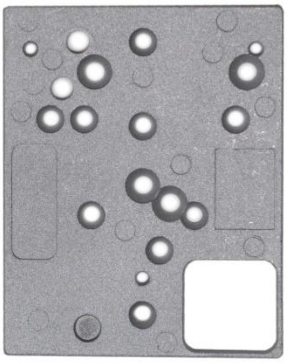


Figure 43: Mounting plate

If the substrate is of metal construction, a safe for example, it is recommended that a specifically designed mounting plate is welded to the safe. These plates can be supplied by the detector manufacturer and provides a flat mounting surface with pre-drilled and tapped fixing points onto which to bolt the detector.

The suitability for use with different substrates and detection ranges claimed vary enormously between makes and models of vibration/shock detectors. It is therefore essential that the manufacturer's technical data are consulted for specific installation guidance.

Adjustments

Vibration detectors need careful adjustment if they are to achieve their optimum detection performance and as with most types of detector the balance between performance and acceptable levels of immunity to false alarm must be found.

The types of adjustment can vary from simple sensitivity switch settings to the accurate tailoring of complex electronic filter response curves to achieve the optimal detection characteristics.

Some detectors have optional software available to aid the installation and commissioning and can include features such as, graphical representations displaying the levels of vibration detected and their frequency distribution. Most will also have soak testing capabilities, a useful feature that can be set to monitor and record vibration levels over several days, enabling the identification of less obvious sources of vibration which could potentially result in false alarms.

Test transmitters can be purchased to aid adjustment during installation. These are also useful when conducting confirmation checks, particularly on sites where significant numbers of vibration detectors are installed. Note however, that the use of such test devices should not replace the need to visit each detector periodically to visually inspect it for signs of damage and to confirm that it remains securely mounted.

Whilst the IDS installer must determine the most suitable adjustment settings for the vibration detector, it is recommended that the security manager records the chosen parameter settings and retains them for future reference. These parameters shall include all hardwired and software/firmware settings, e.g. sensitivity, pulse count setting, filtering attenuation, and material type selection. Such information could become invaluable when attempting to resolve problems should they arise in the future or if the detector should ever be replaced, the original settings will be available.

Known causes of false alarm

To avoid false alarms, vibration detectors must have solid fixings that are secured to a stable mounting substrate. Detectors that have become loose are very likely to create unwanted alarms and are just as likely to miss a genuine alarm event.

The mounting of vibration/shock detectors across differing material types or across joints in the substrate, (such as at the corner of a door or window frame), or across the expansion joint of a wall must be avoided. The movement created through the natural expansion and contraction effects of the joints is likely to result in a false alarm. The movement may be interpreted by the detector as a genuine alarm signature.

It is particularly important to thoroughly survey the premises/areas to be protected and their immediate surroundings to locate and identify all potential sources of vibration that might later cause false alarm problems. Check for the presence of; railway lines, heavy road traffic and low flying aircraft and other intermittent sources of noise.

If a potential source of false alarm is identified it may be possible to eliminate it with the use of selective electronic filtering within the vibration detector. Alternatively, another type of detection technology could be considered.

Avoid installing vibration detectors in areas where there is public access or areas used by staff at times when the IDS is set. The ambient vibrations may inadvertently trigger the detectors.

Additional installation measures may be needed when installing vibration detectors in locations known to have high levels of electrical interference, for example, mobile communication test sites. The use of high quality screened interconnecting cable and additional filtering of the power supply lines may be necessary if problems are experienced.

In high humidity or corrosive environments seek confirmation from the manufacturers of the suitability of their products.

Protecting against attack

Apart from implementing standard precautions, such as the use of supervised alarm and tamper loops and ensuring that any associated junction boxes are adequately protected against tampering, there are no special requirements recommended for protecting vibration detectors against compromise attacks.

If it is considered necessary to locate vibration/shock detectors within a more robust housing offering increased physical protection, take care not to create a resonant cavity within the protective housing that effectively amplifies unwanted noise and vibrations thereby making the detector susceptible to false alarms.

The vibration detector manufacturer may be able to supply a range of optional housings and fixing kits that may help with the installation.

Protective switches

Protective switches are used to sense when a door or window or other type of aperture is opened. They are often used on the final entry/exit doors to signal to the CIE that the user has either entered or has left the supervised area/premises during the IDS un-setting and setting procedures.

Operating principles

Protective switches are available in many shapes and sizes and with a range of operating characteristics to suit a wide variety of applications. The common types of protective switch are listed below:

- **Mechanical switches** comprise a micro switch attached to an actuator mechanism such as a lever or a plunger. All parts of the mechanical switch are housed within a single housing suitable for mounting to a door or window frame. Some are designed for surface mounting, others for concealed flush mounting.

- **Magnetically operated reed switches** are the most common type of protective switch. Supplied in two parts; the magnetically operated reed forming an electrical switch and a magnet.

A pair of electrical contacts on ferrous metal reeds are housed within a hermetically sealed tubular glass envelope. The electrical contacts are normally biased opened, closing when a magnetic field is applied.

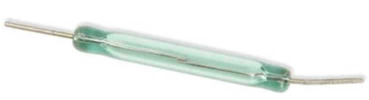


Figure 44: Magnetically operated reed

In use, the switch is attached to the fixed part of the aperture to be protected, usually a door or window frame and wired to the control equipment. The magnet is attached to the moveable part of the door or window.

Opening the door or window moves the magnet away from the reed switch causing the electrical contacts to open, signalling to the control equipment that an alarm event has occurred.

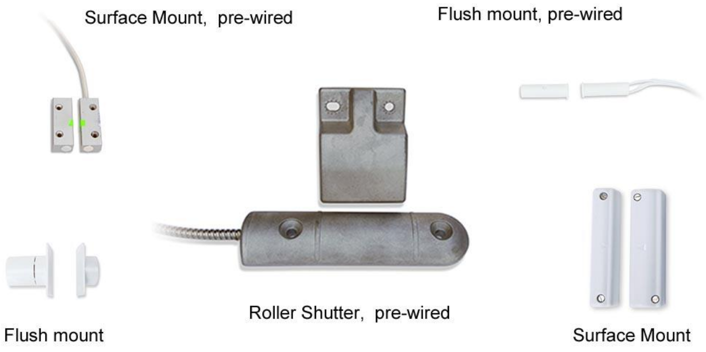


Figure 45: Examples of magnetically operated protective switches

Hall Effect switches are also magnetically operated devices again supplied in two parts; a switch assembly and a magnet. Constructed of solid state semiconductor material there are no moving parts to wear out.

Hall Effect switches (named after Edwin Herbert Hall who discovered the effect in 1879) are mentioned here for completeness. They are available but are not widely used with IDS at present. The main reason for this is that to provide a useable output for connection to the control equipment Hall Effect sensors require additional electronic components. This adds cost when compared with the standard magnetically operated reed switch and hence makes the manufacture of Hall Effect devices less commercially viable.

- **RFID (Radio Frequency Identification Device)** are, at the time of writing**,** in development but unavailable commercially. RFID technology will facilitate the use of an encrypted communication protocol between the fixed and moveable parts of the protective switch which could make for a very secure device that is difficult to compromise.

Mechanical switches

Mechanical switches are used where it is inappropriate to use magnetic types or where the nature of the application requires a bespoke mechanical arrangement. Since mechanical switches normally contain no magnetically operated parts they are resistant to compromise attack by introducing magnetic fields.

Subject to the level of use when in service, they may require frequent adjustment to take up wear on the moving mechanical parts. Regular checks are also required to ensure that the mechanical parts do not stick in the closed position, especially on switches mounted on the lower part of the door frame which can accumulate dirt over time.

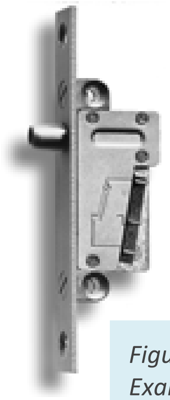


Figure 46:
Example of a mechanical switch

Magnetically operated reed switches

Due to the relatively low cost of the standard types of magnetically operated reed switches these types of protective switch have become the most popular. However, some 'high security' models command higher prices due to the addition of in-built anti-tamper protection measures.

Typically the anti-tamper measures comprise two or more magnetically biased reed switches in addition to the alarm signalling reed switch. The additional reed switches are physically orientated in different positions to each other and to the alarm switch.

The selective positioning of the anti-tamper reed switches ensures that they only operate when a secondary external magnetic field is present, e.g. introduced by an attacker intent on interfering with the operation of the protective switch. The result is a tamper output from the protective switch signalling to the control equipment that a comprise attack has been attempted.

The reliability of magnetically operated reed switches is generally very good however, after many operations their electrical contacts will eventually wear out. Contact resistance measurements made as part of the scheduled maintenance checks should provide warning of impending contact failure.

Application

It is recommended that protective switches are installed in accordance with the manufacturers guidance provided it does not conflict with CPNI advice or compromise security.

The type of protective switch used and the mounting position chosen shall be selected to ensure the aperture (i.e. door or window etc.) cannot be opened too far before detection occurs.

CPNI Protection Levels BASE, ENHANCED and HIGH; an alarm condition shall occur before the gap between the frame and the edge of the door (window or other moveable part) exceeds 20mm.

When protective switches are used in applications required to meet CPNI Class Ratings an alarm condition shall occur before the door/window etc. clears the frame, allowing no opportunity for an intruder to see into the protected area.

Note: if the operating distance is made too small, the tolerances associated with the normal movement of the door (window or other moveable part) may lead to false alarms.

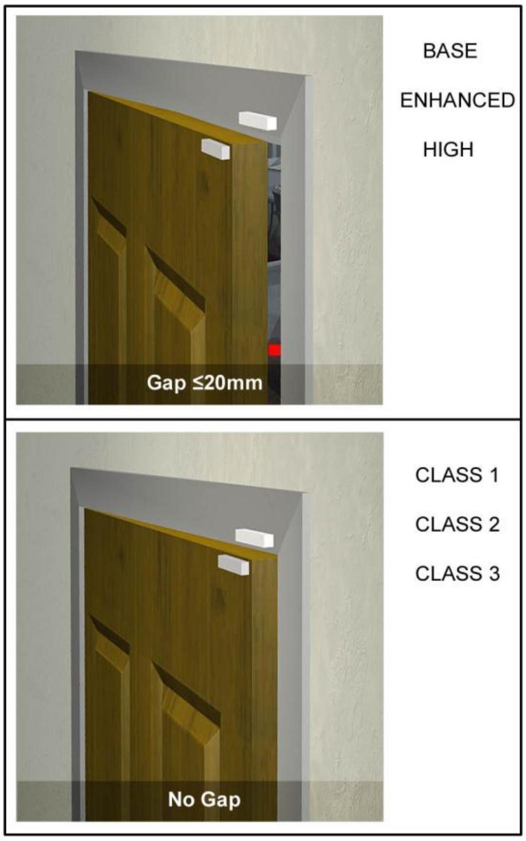


Figure 47:
Acceptable range of opening movement

Checks should be made to confirm that it is not possible to create an alarm when the door (window or other moveable part) is closed and deliberately moved within the constraints of the catches or locks.

Protective switches must be separately identifiable at the CIE. The only permitted exception is where two protective switches are used on the adjacent leaves of a double door, they can be considered as being two sensors of a 'single device'.

Magnetically operated protective switches can also have novel applications such as, sensing the removal of a specific asset. Placing the magnet on or within the asset and programming the detection circuit to 24 hour monitoring will warn if the asset is moved away from the protective switch.

Adjustments

Other than slider plates and shims to aid adjustment during installation, protective switches normally have no other adjustments except perhaps at Protection Level BASE if a wireless device is used. There is normally a switch for selecting the desired radio channel.

Mechanical protective switches may require realignment periodically during maintenance visits to compensate for any physical wear.

Known causes of false alarm

The most likely causes of false alarm from a protective switch are due to excessive movement of the surfaces to which the switch is secured, or the protective switch working loose from its mountings.

As reed switches get older and eventually wear out their electrical contacts may develop high resistance which if not identified during maintenance, could result in a false alarm.

More frequent checks of protective switches mounted on heavy doors will be necessary. This is because the high energy shock pulse produced when the doors are slammed shut could cause the switches to fail earlier than might normally be expected.

Protecting against attack

Mechanically operated protective switches should be positioned such that access to them cannot be gained from outside the supervised area/premises when the aperture is closed.

All magnetically operated protective switches should incorporate anti-tamper measures such that the deliberate application of a secondary external magnetic field shall cause an intruder alarm or tamper alarm condition.

Where supervised loop wiring* uses end-of-line resistors, protective switches incorporating the corresponding value resistors should be used. The end-of-line resistor must be fitted into the protective switch enclosure in order to protect the full cable length. The practice of fitting the end-of-line resistors in the protective switch joint boxes should be avoided. In any event all joint boxes should be fitted with tamper detection devices.

If and when available, RFID based encrypted protective switches might also offer additional resistance to tampering.

** Further information about supervised loop wiring and detection circuit supervision is provided on page 95.*

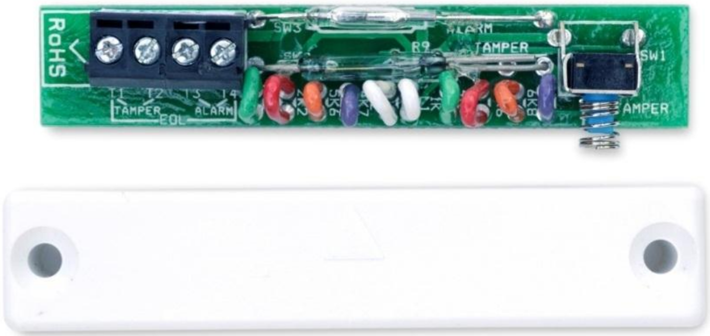
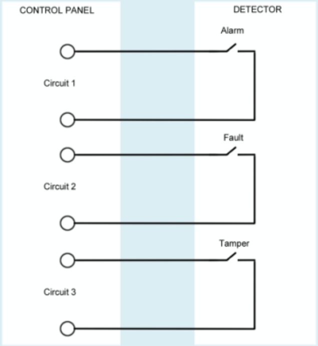


Figure 48: Selectable end-of-line resistor combinations. The coloured wire links inside the protective switch allow for the selection of end-of-line resistors matching the CIE configuration to provide a supervised interconnection.

Detection circuit supervision

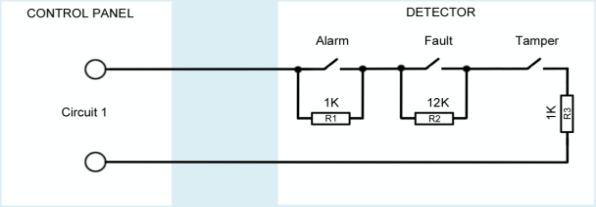
The terminology associated with the supervision of detection circuits used by different manufacturers can be confusing. Following are examples of common configurations and the CPNI grading recommendations;

Figure 49 Closed Circuit Loop



Closed Circuit Loop, Continuous Closed Loop, Normally Closed Loop. These are terms for conventional wiring where there is a continuous closed loop for the alarm circuit and another separate continuous closed loop for the fault circuit and a further separate continuous closed loop for the tamper circuit (Figure 49). Repeated for each detector. The switches shown as representing the alarm, tamper and fault outputs are closed when the detector is in the normal quiescent (i.e. non-alarm) condition. This configuration can be used at Protection Level BASE and ENHANCED or Class Rating 1.

Figure 50 Fully Supervised Loop

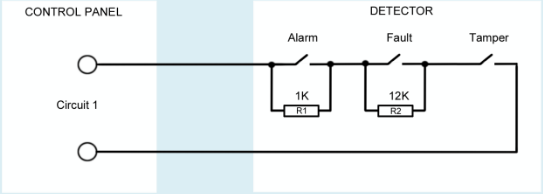


Fully Supervised Loop, Balance Loop, Triple End of Line Loop.

Resistors located in the detectors set the value of loop resistance. In accordance with Ohms Law the resistance is proportional to the flow of electric current in the loop. The control panel monitors the flow of current. When one or more of the outputs opens the loop resistance changes.

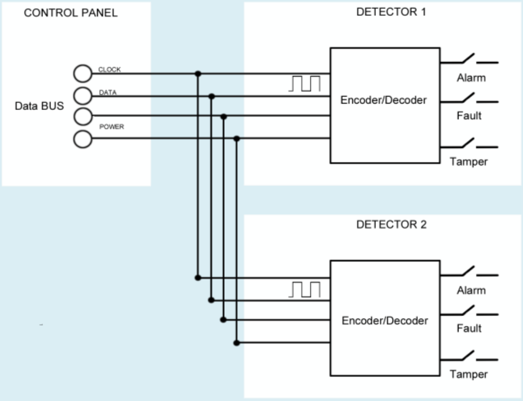
To ensure the loop is correctly supervised the resistors must not be located inside the control panel. This method of circuit supervision can be used at Protection Level ENHANCED and HIGH or Class Rating 2.

Figure 51 Partially supervised loop



A variation of the fully supervised loop is the partially supervised loop or dual end-of-line loop, (Figure 51). The method of operation is very similar to that described above, but with no series resistor R3. This method of circuit supervision should not be used.

Figure 52 Addressable data BUS



IDS incorporating addressable data BUS type (Figure 52) interconnections can offer a robust method of communication. Coded or encrypted data packets are transmitted over the BUS to and from the detectors and other peripheral devices. Frequent polling is used to confirm the availability of the interconnections. Alarm, tamper and fault events interrupt the polling cycle for immediate action.

The level of security integrity of the transmitted protocols varies widely between makes and models of IDS, but those deploying AES encryption can be made very difficult, if not impossible to compromise. This method of circuit supervision can be used at Protection Level HIGH or Class Rating 3.

Active Infrared Detectors (AIRs)

Active infrared detectors provide one or more beams of infrared that can be aligned to create a 'detection barrier' invisible to the human eye. If the beams are interrupted, for example by an intruder passing through them, the loss of infrared signal at the receiver is detected and an alarm created.

Operating principles

As the name suggests, active infrared beams are an ‘active’ type of device meaning that they emit infrared energy, as opposed to passive infrared detectors that only receive infrared. The operating wavelength is different too, typically in the 800-980nm waveband, which is beyond the response range of the unaided human eye.

Operating distances of AIR detectors intended for indoor use are available from 4m to 200m and possibly greater. Devices capable of operating distances greater than 5m use collimating lens and/or mirrors to intensify and focus the projected infrared beams.

The electronic circuitry is generally in two parts; a transmitter that emits modulated bursts of infrared light and a receiver with optics and circuitry to collect and decode the modulated signal produced by the infrared light.

There are 3 basic configurations:

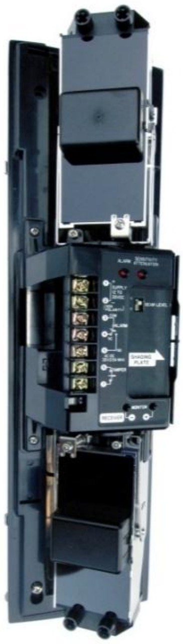


Figure 53: Active infrared beam receiver with housing cover removed

1) Reflected: The transmitters and receivers are located within the same housing. They work by shining the infrared light towards a reflector placed some distance away. The reflector bounces the infrared energy back to the receiver. The infrared beam is broken as the intruder passes between the detector and the reflector. Whilst commonly available, this configuration is not suitable for security applications above Protection Level BASE.

2) Separate transmitter and receiver pairs: The transmitters and receivers are located in separate housings installed some distance apart. One or more infrared beams are emitted and aligned with the optics of the receiver. An intruder moving between a transmitter and receiver pair obscures the beam(s) causing the receiver to immediately enter an alarm condition.

3) Multiple beams/towers: Multiple beams/towers are combinations of the above configurations generally made up of two or more transmitter and receiver pairs (but can also be the reflected type). Mounted together, the multiple transmitter/receiver pairs provide an array of infrared beams which can be positioned to create invisible detection barriers. These can be configured to generate an alarm if one or more of the beams are interrupted.

Application

Common applications include:

- detection within the internal perimeter of the supervised area/premises;
- detection of movement through doorways and window apertures;
- detection within ceiling voids;
- detection of breaches of exterior walls, e.g. the forcible penetration and subsequent entry by the intruder will interrupt the infrared light beams and signal an alarm.

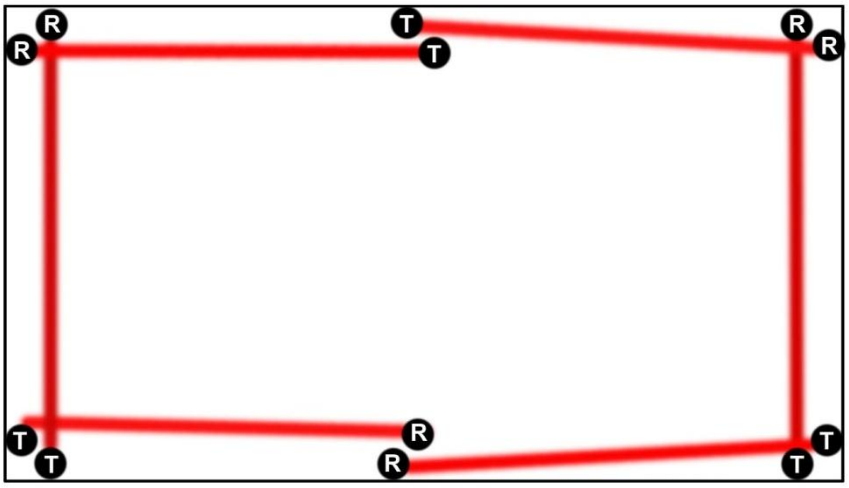
Running AIR detectors close to metal clad walling can be problematic. When the cladding is exposed to strong sunlight the heating effects will distort the infra-red beams and sometimes cause an alarm. This phenomenon can also be observed by the human eye when light transmissions close to the hot surface take on a shimmering effect.

Suitably weather proofed AIR detectors may also be placed outdoors across window apertures on the perimeter of the supervised premises to provide early warning of an intrusion attempt. These are categorised as components of perimeter intruder detection systems (PIDS) and are not specifically included within the scope of this guidance.

It is however worth mentioning that AIR detectors designed for use outdoors can be installed indoors. Outdoor AIR detectors are similar in operation to those designed for internal use but they have weather resistant enclosures and often incorporate internal heating elements. The heating elements prevent condensation forming on the optical assemblies during rapid transitions of temperature. The presence of condensation will attenuate the infrared signal and possibly lead to a false alarm. Heater elements can also be used with indoor AIR, for example in an unheated warehouse where the risk of condensation is also likely.

The transmitter and receiver pairs of multiple infrared beams should be positioned in an alternating configuration (Figure 54) and set to a different operating channel to reduce the possibility of cross beam interference, (that is, when the multi-channel feature is provided).

Figure 54: Alternating pattern to avoid cross beam interference



Adjustments

Depending on the make and model of AIR, several adjustments may be available, such as:

- Sensitivity
- Response timing
- Number of beams to be interrupted
- Operating channel

The optical assemblies must have controls to enable the precise alignment of the transmitted infrared beam with the corresponding receiver.

Alignment methods vary, from the use of simple fiducial marks and telescopic sights to laser-based pointer systems.

Known causes of false alarm

Early designs of AIR detectors were basic devices without too much in the way of signal processing, in contrast modern types have multiple features designed to reduce the possibility of false alarms.

Modulating the infrared emissions prevents extraneous light (e.g. bright sunlight) from saturating the infrared beam receiver, effectively blinding the detector.

Adjustable timing circuitry allows the response time associated with the interruption of the beam to be set to ignore moths and other flying insects, possibly even birds if they become trapped within the supervised premises after the IDS has been set. Generally interruptions of 20ms or less are ignored.

The gradual build-up of dust and/or dirt on the front of the detectors may eventually attenuate the infrared signal sufficiently that an alarm results. As the infrared signals become increasingly attenuated through the build-up of dust, the detectors may appear more sensitive and less tolerant of sources of disturbance within the environment that otherwise would be ignored.

As mentioned previously, condensation settling on the optics can be avoided by fitting heater elements inside the detector.

The detectors must be securely fastened to their mountings; any movement will misalign the transmitter and receiver resulting in either a fault or an alarm condition.

Building movement may contribute to false alarms. Some structures move over time so the AIR detectors might require periodic checks and if necessary re-alignment. Movement may also be part of the building design, e.g. very tall towers are designed to sway so as to absorb the effects of wind loading. Where excessive movement is known to be present AIR detectors should not be used.

Alignment checks of AIR detectors should be included as part of the schedule maintenance routine.

Detectors which alarm upon the interruption of only a single infrared beam are more likely to false alarm if rodents, small animals or birds are present. Configuring the detector to alarm only after two or more infrared beams have been interrupted simultaneously will significantly reduce the risk of unwanted alarms. Obviously, care must be taken not to compromise the security by creating a large a gap in the detection coverage if this method is used.

Protecting against attack

All AIR detectors should incorporate back tamper and have the means to detect the removal of covers. It is good practice to position the AIR detectors in such a way that each pair of beams is protected by another, see the configuration of Figure 55.

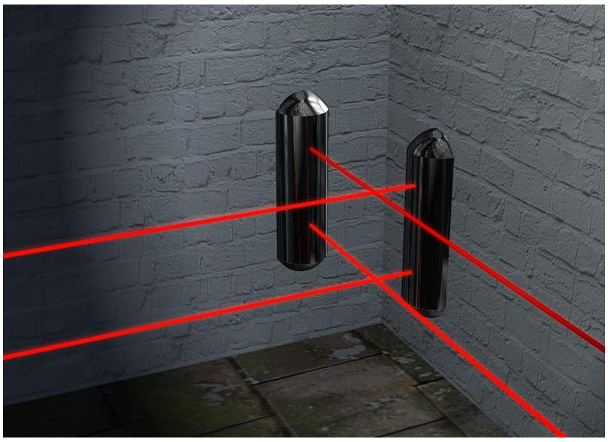


Figure 55: Recommended AIR detector configuration

In some circumstances this is not possible, e.g. a single beam set across a window or a door.

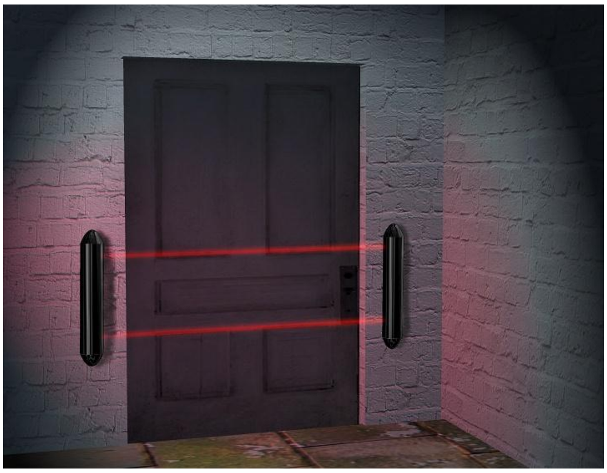


Figure 56: A single beam set across a door

If the threat level suggests there is a genuine risk that the detectors might be exposed to compromise attack, the use of AIR detectors incorporating coded supervisory circuitry that monitors the strength of the received infrared signal is advised. These detectors will sense and warn of small changes in the received signal levels, either a decrease or an increase in level. Such features make it difficult for a successful bypass attack to be orchestrated using secondary transmitters or prisms to create alternate beam paths.

Some AIR detectors can also have an encrypted signature superimposed on the infrared transmissions. This adds an extra level of security to prevent substitution attacks should a second AIR transmitter of the same make/model be introduced. Encrypted infrared beams require the installation of interconnecting cables between the transmitter and receiver so that the pair remains synchronised.

Annex B: Warning device types

Audible warning devices

An audible warning device produces a distinctive varying sound output, which is specifically designed to attract attention. Audible warning devices are fitted where it is considered appropriate either; to warn on site personnel of an intrusion or attempted intrusion, or to scare away the intruders.

Whilst the traditional mechanical bell types are still available the most popular type of audible warning device is the electronic siren, comprising a speaker or horn assembly electrically coupled to a tone generator and amplifier.

All audible warning devices sound in response to a signal from the control panel although the exact method of operation varies. The following descriptions are based on commonly used terms that whilst the names are not entirely applicable to modern technology, they are frequently used within the security industry.

Where audible warning devices are located outside of the supervised area / premises the use of monitored or supervised interconnections between the CIE and warning device is necessary to detected and signal a tamper alarm in the event of attempts to prevent the notification signal reaching the warning device.

⚠ Care is required when specifying audible warning devices for use in enclosed spaces as loud sirens can cause noise induced hearing loss, which is irreversible. It is therefore strongly recommended that appropriate health and safety guidance is followed. Advice can be obtained from the Health and Safety Executive website at www.hse.gov.uk.

High output external sounders, such as the Klaxon Master Blaster™ which is mains powered, should only be used in large open spaces and normally where premises are isolated from neighbouring properties, such as farms, etc.

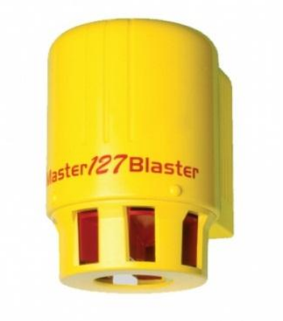


Figure 57: A Klaxon Master Blaster™ 127db

Self-contained bell (SCB)

The terms **self-contained bell** and **self-actuating bell** are legacies from the time when bells were frequently used in warning devices. The term is slowly being replaced by SCS - self-contained sounder (and SAB: self-actuating bell, see below).

SCBs are warning devices which incorporate tone generator circuitry and a standby battery recharged from power supplied (normally) by the control panel. In the event of an alarm condition and the warning device sounds, power is taken from the warning device battery so as not the overload the control panel power supply in installations where the current available to supply auxiliary equipment is limited. Commonly SCB are used where more than one audible warning device is required.

Self-actuating bell (SAB)

Warning devices that incorporate tone generator circuitry and a battery recharged from power supplied (normally) by the control panel. In the event of an alarm condition and the warning device sounds, power is taken from the control panel supply.

Should the interconnection between the CIE and warning device be severed (e.g. if attacked) the warning device standby battery takes over the supply of power to sound the alarm. Some types of SAB produce a lesser volume of sound in this mode because the battery used is not capable of delivering the required current to run the sounder at full volume.

Often warning devices incorporate a switch allowing the installer to select SCB or SAB mode of operation. SABs and SCBs are suitable for locating outside the supervised area. The use of polypropylene housings/covers should be avoided as they quickly degrade when exposed to prolonged sunlight.

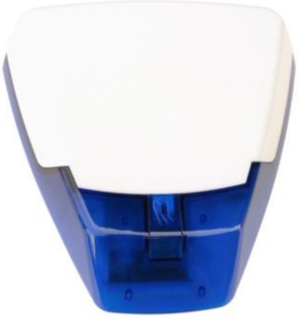


Figure 58: External warning device (SCB/SAB operation selectable)

Remotely powered warning devices

Warning devices that incorporate tone generator circuitry and are powered by the CIE.

Should the interconnection between the CIE and warning device be severed (e.g. if attacked) the warning device stops sounding. It is recommend that these types of audible warning device are located within the supervised area, although for commercial applications they are permitted outside under the circumstances defined in BS EN 50131-1[10] Table 10.

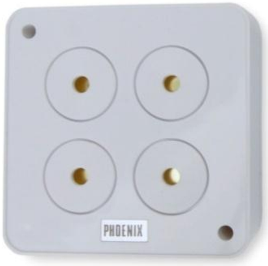


Figure 59: Remotely powered warning device

Speaker/Horn (warning devices without an integral tone generator)

To sound an alarm, a modulated tone must be supplied, usually generated by the CIE. These types of audible warning device are intended for installation within the supervised area.

Voice alarms

Voice alarms provide a pre-recorded spoken annunciation of an alarm condition or other type of message; these are particularly useful if it is necessary to give commands to on-site personnel or even intruders. Voice alarms are sometimes used in conjunction with fire and/or evacuation systems and with options for multi-lingual messaging.

Such devices can be self-contained or driven directly by the CIE. Consideration should be given to the level of intelligibility required of the spoken message and the acoustics of the service environment.

Figure 60: Horn assembly

Warning devices used outdoors

Warning devices intended for outdoor use must include suitable weather proofing. The warning device should not be the primary means of alert, all alarm activations must be monitored at a guard monitoring terminal. Tamper protection should be provided so that the enclosure cannot be opened without the use of a tool. Additional tamper detection should be installed to detect opening of the enclosure and to detect the removal of the unit from its mounting surface.

The selection of an appropriate warning device will in part depend on the level of ambient noise in the service environment. As an example a device with a mean acoustic output of approximately 100 dB(A) when measured at a distance of 1m, should be suitable for most applications with an ambient noise level of between 60-80 dB(A).

All external audible warning devices must comply with Environmental Protection Act 1990-s79-80 Statutory Noise Nuisance and the Clean Neighbourhoods and Environment Act 2005[26]. In practice this means the sound emissions of external sounders must automatically shut off within 20 minutes.

To fully comply, the timing device must be incorporated within the external sounder to ensure the sound emissions stop even if communication with the control panel is lost, e.g. the interconnecting wires are broken. The permitted frequencies of the acoustic output may also be subject to variation depending on local or national requirements. Generally the equipment manufacturer should be able to advise.

Visible warning devices

Visible warning devices comprise a light source such as a flashing array of high intensity light emitting diodes (LEDs) or a Xenon strobe. They are used to provide visible indication of an alarm condition. Available as part of an audible warning device or as a standalone component. Standalone visible warning devices are not normally supplied with integral tamper protection.

Visible warning devices installed outside the supervised premises are often configured to remain illuminated after the sounding duration of the audible warning device has timed out. This indicates to users prior to entering the supervised premises that an alarm has occurred during the set period.

⚠ Caution is advised when using visible warning devices that continue to operate after the audible warning devices time out, as the flashing beacon also signals to an intruder that the premises are not being closely managed. Many insurance companies now insist on this feature being disabled.

CPNI
Centre for the Protection
of National Infrastructure

www.cpni.gov.uk